Cybercrime Checks Into Hotels: 
*Cybersecurity Threats and Countermeasures*

Basic Security Concepts

HOST 100
Career & Customer Service Skills
Learning Objectives

• Upon the conclusion of this module, the student will be able to:
  – Identify the effect that cyber warfare and cybercrime can have on society and an organization.
  – Describe the impact of cybercrime in hotels and resorts.
  – Explain the trade-off between key security properties and usability.
  – Identify the basic concepts of threats, vulnerabilities, attack vectors, and risk.
  – Explain risk-handling procedures essential to providing quality service to guests
What Do These Hotels Have In Common?
Cyber Warfare

- Cyber warfare involves actions by a nation-state or international organization to attack and attempt to damage another nation’s computers or information networks through, for example, computer viruses or denial-of-service attacks
Cybercrime

• Unlike cyber warfare activities, cybercrimes are malicious activities that are often financial in nature
  
  - Credit card theft (most often large-scale)
  - Cyber extortion (ransomware attacks)
The War is On: Cybercrimes in Hotels & Resorts

“Marriotts among hotels in 8-state-wide data breach, manager says”

“Card Breach at Trump Hotel Properties”

“Hilton Acknowledges Credit Card Breach”

“Hyatt Hotels Discovers Card Data Breach at 41 Properties”

“Innovative Cyber Criminals Hack Austrian Hotel”

“Trump’s Hotel Chain to Pay Penalty Over Data Breaches”
Guest Expectations

Security
• Physical building

Data
Credit card
Contact details
Travel plans
Air miles
Birthdays
Personal preferences
Guest Expectations

Personalization of Service

Making connections

“Quality” service

Human Element
Hotel Targets

• Restaurants
• Gift shops
• Point-of-Sale (POS)
• IT systems
• Guest registration databases
• Digital keys
• Wi-fi networks

• Malware
  Cardholder’s name, number, internal verification code

• Implications
  Brand reputation & image

• Challenges

Many touchpoints!
Security Trade-Off

• In addition to the security challenges previously addressed, **there is always a trade-off between security and usability.** As security services, such as those providing for confidentiality, integrity, and availability, are implemented, system performance and accessibility suffer.
Lab Exercise

Security Trade-Off

• You are a front office agent and Mr. Smith is requesting another key to his room because he misplaced it. He just came from the pool and has no ID with him.

What should you do?
Security Threats

• A security threat is the potential for an event to occur that would negatively impact security.

• The potential to cause damage to a system is considered a threat.

• There are three types of threats:
  – Natural events (also called “Acts of God”)
  – Human error (accidents)
  – Attacks – attacks require malicious intent, so must be caused by people who would circumvent or violate security.
Attack Vectors

• **Attack vectors** are the methods, or path, that the attacker (threat actor) will use to attack. It is the path that they will take to take advantage of a vulnerability.

• As an example, attackers will often use social engineering techniques, such as phishing, to attack a network.
Social Engineering

- Manipulate people to give up confidential information
- Easier to exploit natural inclination to trust rather than hack software

- Attacks - Example
  
  Emails from “friend” or “trusted source”
  
  *Contains link, download, etc. with malicious software embedded*
Lab Exercise #2 - Attacks

Social Engineering Attack

• Using a compelling story or pretext to take advantage of trust and curiosity, write a convincing email (as a guest) that asks your favorite staff member to check out a link or download a file (malicious software embedded).

• Discuss email policies that should be in place for staff.
Risk

- **Risk** is the degree to which an organization is exposed to the threat, and takes into consideration the **likelihood** and **impact** of the threat being realized.
Risk Handling Techniques

• Risk handling is the process of managing risk so that either the likelihood of the threat occurring is reduced, or the impact is reduced.

• Risk handling techniques include:
  – Risk Avoidance
  – Risk Mitigation
  – Risk Acceptance

• The degree to which an organization “accepts” risk (chooses to do nothing) is based on their risk tolerance. A “risk averse” organization will be more likely to implement security controls, even if they are more costly than the event.
Risk Handling – Management’s Role

Develop security procedures

Train

• Secure systems
• Password policies
• Recognize attack vectors

Enforce compliance with security rules and policies

Prepare response team
Catalyzing Computing and Cybersecurity in Community Colleges

Is funded by a National Science Foundation grant and is located at Whatcom Community College

237 West Kellogg Road
Bellingham, WA 98226

www.C5colleges.org