DATA SECURITY: HOSPITALITY

Strategy for data protection and regulation compliance

PRODUCED BY:
HFTP
Hospitality Financial and Technology Professionals

DATA SECURITY: HOSPITALITY

TEAM

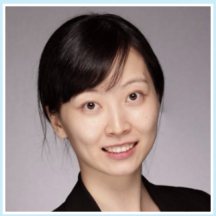
Lead Author
Tanya Venegas, MBA, MHM, CHIA is the executive director and HFTP Fellow at the HFTP Americas Research Center based at the Conrad N. Hilton College, University of Houston in Houston, Texas USA.

tanya.venegas@hftp.org

Project Manager
Eliza Selig is the director of communication for Hospitality Financial and Technology Professionals (HFTP) in Austin, Texas USA.

eliza.selig@hftp.org

Contributor
Evita Ma is the executive director at the HFTP Asia Research Center based at the Hong Kong Polytechnic University in Hong Kong.



Contributor
Sunny Wang is a graduate assistant at the HFTP Americas Research Center based at the Conrad N. Hilton College, University of Houston in Houston, Texas USA.

Executive Editor
Nick Price is CEO at Netsys Limited Technology and a director on the HFTP Global Board.

Executive Editor
Alvaro Hidalgo is managing partner at FIRSTLOGIC Consulting and chair of the HFTP GDPR/DPO Task Force.

HFTP
Hospitality Financial and Technology Professionals

Global Headquarters
11709 Boulder Ln, Ste 110
Austin, Texas 78726
+1 (512) 249-5333 • (800) 646-4387 *(US only)*
www.hftp.org

FOREWARD

HFTP ASSISTS WITH DATA SECURITY RESOURCES

Many governments across the globe, such as the European Union and China, are responding to the cybercrime wave with strict regulations that push companies to enact protocols which will protect the consumer (i.e. your guests). And so, with these new tech tools in our arsenal, comes the important task to secure against infiltration, a top priority for IT teams. IT security has become one of the biggest responsibilities of the tech team, with many resources dedicated to protecting customer data and the systems we use to run our operations.

HFTP aims to provide valuable resources to the hospitality industry to help navigate the changing business environment and data protection is a particularly pressing issue for hospitality. The lodging industry is a top target for cyberattacks, as hotels collect large amounts of personally identifiable information — gold for cybercriminals. What follows is a comprehensive report on data protection for the hospitality industry. It provides knowledge and understanding of security practices and regulations as they stand today. Readers will learn about safeguards they can implement in their businesses today and tips on how to continuously improve security. Technology is changing at a rapid pace and hospitality businesses big and small must be ready for cybersecurity threats both now and in the future.

FRANK WOLFE
CEO • HFTP

A CYBERSECURITY PLAN IS A BUSINESS IMPERATIVE

Since I spoke at HITEC several years ago, cyberattacks have dominated global headlines and caused every person and every company to evaluate their cyber health. The truth is that cybercrime is rising dramatically and everyone is a potential victim. Few are lucky enough not to have been affected already. Massive data breaches like Equifax, Target and Facebook prove that taking your digital health seriously is critical in our increasingly interconnected world.

Every company, regardless of size or revenue, must act now. For corporations with limited resources, the thought of diverting funds from customer experience — the lifeblood of the hospitality industry — seems impossible or at the very least foolish. I get it — any dollar you spend on security is a dollar you cannot allocate to service improvements, better hotel rooms or guest perks. My best piece of advice I can give you is to determine your two most important assets. What are your crown jewels? Most hotels would cite their guests' personally identifiable information and customer payment data. Develop a plan now to safeguard those two assets, then simulate a digital disaster, so you know who is in charge when the inevitable hits. Seek qualified partners and review your agreements with them to understand where responsibility lies. Focusing on cybersecurity shouldn't feel scary or daunting. If I may be so bold, designing a cybersecurity plan is a business imperative. The unfortunate reality we live in is that a cyberbreach is no longer an IF, but a WHEN. The steps outlined in this report provide a great starting place for any hospitality organization to assess their cybersecurity. Stay safe!

TERESA PAYTON
President & CEO • Fortalice Solutions

Payton served as the first female chief information officer at the White House, overseeing IT operations for President George W. Bush and his staff. She is the author of several publications on IT strategy and cybersecurity and a frequent speaker on IT risk. In 2014 she co-authored, with Ted Claypoole, the book Privacy in the Age of Big Data: Recognizing Threats, Defending Your Rights, and Protecting Your Family. *Payton is the Closing Keynote speaker at HITEC Houston on Thursday, June 21, 2018.*

INTRODUCTION

Reports of hackers breaching systems is a regular occurrence. The hospitality and tourism industry is a major target due to the amount of information processed through its systems on a daily basis. Globally, the World Tourism Organization (WTO) reported there were 1,322 million international tourist arrivals, overnight visitors, in 2017[2]. Looking into the future, by 2030 the WTO estimates there will be approximately 1.8 billion international tourist arrivals. These numbers seem staggering when you think of the amount of data which is being collected, processed and must be safeguarded. In addition, the types of information targeted are wide-ranging as personally identifiable information (PII) eclipses payment data in value. What would happen if this data was compromised? Not only would the company have to sort through regulatory and reporting standards such as the EU GDPR and payment industry standards (PCI DSS), but the organization would also need a solid response plan in place to prevent harm to its reputation.

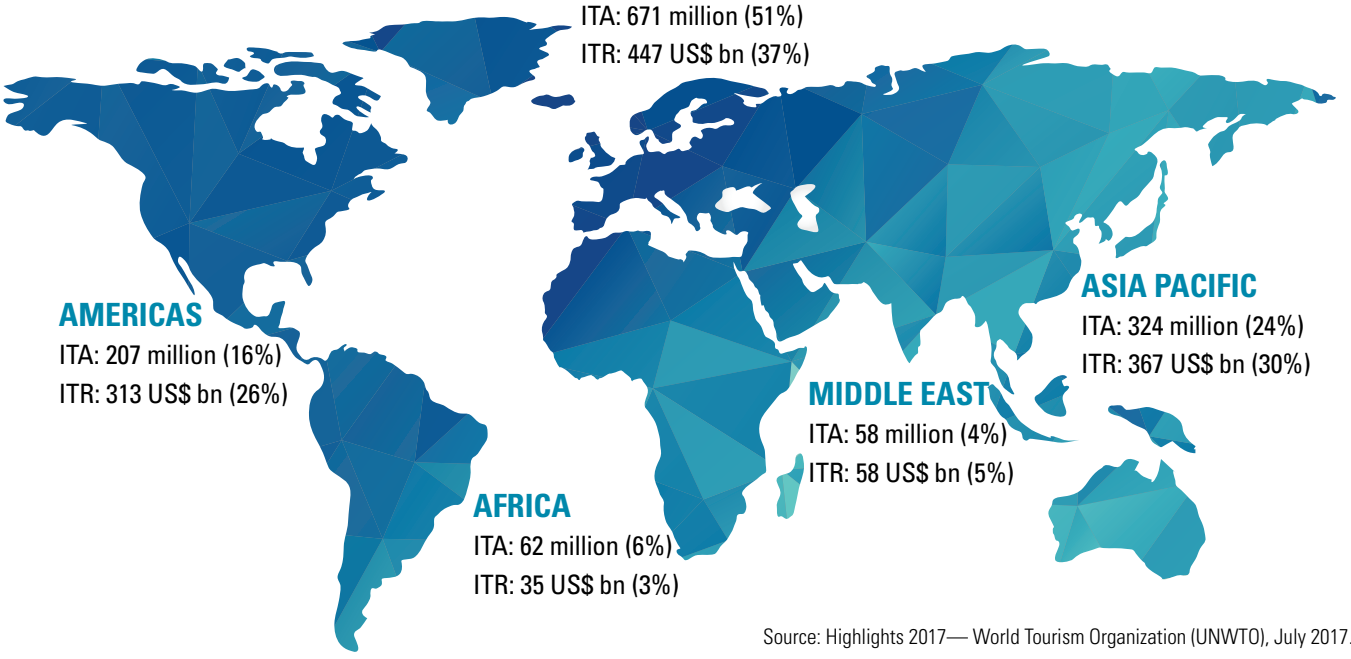
Why is the Hospitality Industry a Primary Target?

There was a day when the hospitality and tourism industries operated off of the grid, dealt only with paper and lived outside of the digital realm; but, times have changed and we are not living in that world anymore. Guests demand hospitality organizations maintain their profile which may include credit card data, PII and preferences such as the type of pillow they desire, their favorite table while dining at the country club or preferred seating options while flying. It is a balancing act, traversing through cybersecurity measures, legal regulations and guest preferences to set your property apart from the competition.

The hospitality industry is unique in many aspects which creates a challenge when organizing and safeguarding valuable company data. First of all, in many cases, payments are not made by guests until the services are rendered. For example, most rental car transactions or hotel payments are not processed until the guest picks up their rental car or checks into a hotel. Therefore, payment information must be held for a greater length of time than in many other industries. For this reason, multiple security measures must be put into place to protect this data. The National Institute of Standards and Technology (NIST): U.S. Department of Commerce developed comprehensive guidance on securing property management systems in the hospitality sector. These guidelines

INTERNATIONAL TOURISM 2017

International Tourist Arrivals (ITA): 1,322 million
International Tourism Receipts (ITR): US$1,220 billion



Source: Highlights 2017— World Tourism Organization (UNWTO), July 2017.

INTRODUCTION

promote and provide multiple security layers which are recommended to secure systems and connections including "point-to-point encryption, data tokenization, multifactor authentication for remote and partner access, network and user behavior analytics, and business-only usage restrictions."[4]

Data security ownership and responsibilities in the hospitality industry, particularly in the lodging segment, are not cut and dry due to the various organizational structures in ownership, property management, franchises and brand management. Depending on the structure and contractual agreements, the responsibility of data management and ownership can be as complex as a spider web. For example, a hotel may be independently owned with a franchise agreement and managed by a third party. In the case of credit card processing, contracts with the credit card processor may be signed by the management company who then could be liable for any data breaches; but, the management agreement may indicate otherwise. The management agreement could stipulate that the data belongs to the hotel owners leaving them responsible. It all depends on the contractual agreements to determine who owns the data.

In addition, because of the unique operating structure, controlling systems and setting security measures is very complex. The ownership and operational structure often places greater control at the property level, with the ownership and management, leaving less control with the brands; but, the brands are often at the greatest risk of harm to their reputation. Brands can promote data security best practices, but that does not mean property owners and management companies will always follow their sage advice. Also, it is not only about data breaches at a single hotel, in this interconnected world a breach at one hotel can lead into the systems at the corporate center compromising even more data.

TARGETED DATA

Information Valued by Hackers

Cybercriminals target data which has the most value to them, whether the data is traded or sold on the black market, or held for ransom. The following are the types of data collected by hospitality organizations which must be protected.

CREDIT CARD INFORMATION: Organizations have struggled with protecting credit card data for decades. Strides have been made in this area to protect credit card data, with the PCI Security Standards Council leading the way. This data is becoming harder for hackers to capitalize on as credit card organizations have instituted stronger safeguards and cards can be quickly canceled when a breech is exposed.

PERSONALLY IDENTIFIABLE INFORMATION (PII): The value of PII has grown in the marketplace; therefore, laws such as the EU GDPR are being set in motion to help protect this data. With PII, criminals can gather valuable data to draw from a victim's bank account, take over an identity and purchase items under an assumed identity.

COMPANY INFORMATION: Access to company information and systems is also a valuable target to criminals. If hackers gain access to a company's system, they can use confidential information to blackmail a company or hold their data for ransom. In addition, criminals could also gather valuable employee data and threaten individuals working at the company.

How Do Organizations Secure Systems and Safeguard Data?

During the January 2015 World Economic Forum, John Chambers, former CEO of Cisco stated, "There are two types of companies: Those who have been hacked, and those who don't yet know they have been hacked."[5] Many organizations are spending millions on data protection and cybersecurity. According to Gartner, worldwide spending on security services, including consulting and outsourcing, was estimated to total US$51.6 billion in 2017. When you add in infrastructure protection (US$15.5 billion), network equipment (US$10.5 billion), consumer software (US$4.6 billion), and identity access management (US$4.2 billion) the overall total amounts to US$86.4 billion being spent on technology security in 2017. These numbers are staggering and will continue to grow into the foreseeable future with Gartner estimating US$108.2 billion will be spent on technology in the year 2023.[3]

In order to prevent data loss, whether it be company data, marketing data or personnel information, a solid plan must be in place. There are several major areas which must be addressed when developing a comprehensive plan: identify the data at risk, develop a plan to protect the data, detect threats, respond appropriately if a breach is detected and trigger recovery efforts if a breach occurs.[6]

DATA SECURITY

Step 1. Identify

The first step in protecting a business from a data breach is determining the types of data which need to be safeguarded. This data would include information that is central to the core operations of the business and would fetch a high payout for cybercriminals. According to the *2018 Verizon Data Breach Investigations Report*, in the accommodation and food services sector, payment data received the greatest attention with over 90 percent of all data compromises involving payment card data.[7] An interesting statistic to note as overall PII is overtaking the highest-value target spot; payment information is still a get in the hospitality arena.

Once all systems have been analyzed and valuable information has been identified, the work is not complete. A detailed listing of the data must be developed, mapped and updated on a regular basis. The listing should include data and technology assets in an inventory list and should note where data and technology are stored and who has access to both. In addition, multiple copies of this document should be stored securely, including backed up off-site.[6]

Step 2. Protect

According to the *Random House Dictionary*, to protect is to defend or guard from attack, invasion or loss. The *Collins English Dictionary* provides a similar definition, to defend from trouble, harm or attack. What comes to mind when you think about these terms: attack, invasion, harm and defend? These are all terms which would describe a battle; therefore, in this step of the process, business are preparing for battle by defending their assets and training their troops.

Training employees is a critical key in protecting a company from a cyberattack. Employees are the first line of defense and they must be trained and aware of the various types of attacks which can be perpetrated against the organization. Hacking and malware account for the majority of breaches in the accommodations and food services industries.[7]

Step 3. Detect

Detecting a cybersecurity incident early is key to mitigating the long-term impact. In many cases, businesses are unaware of cybersecurity breaches for days, weeks or even months after their systems have been breached. Data breaches can occur in many different forms. It is important for a business to be aware of the different types of breaches to prepare for prevention and detection. In the accommodations and food services industries, most attacks involved malware and hacking threats. [7]

BREACH DETECTION

USE SECURITY UTILITIES TO BE ALERTED TO SUSPICIOUS ACTIVITIES, AND FOLLOW-THROUGH WITH AN INVESTIGATION

" Better use of available security tools such as **advanced threat detection (ATD)** and **file integrity monitoring (FIM)**. ATD monitors system and network activity for traces of suspicious activity. FIM monitors for changes to the operating system and applications files that should not change.

" Automated monitoring utilities such as these must be combined with an effective **security information and event monitoring (SIEM)** solution that monitors system and event logging data from multiple sources and provides actionable alerting to appropriate staff. Finally — and this has been missing in several incidents — qualified security specialists must actually be reviewing and responding to alerts from these monitoring tools."

Ron Hardin
Principal, RonHardin.TECH Consulting

Strategically, there are several ways companies can prepare and plan for detecting breaches within their operations. Businesses must know which threats are applicable to their business and use the best data protection products, practices and services to help monitor and detect any possible intrusions. Again, training is a key aspect in detecting potential breaches. Employees should be trained to recognize and report any unusual activities to the appropriate individuals within the organization.

Step 4. Respond

Unfortunately, even with the best risk control practices, there is still a possibility for information security incidents such as data breaches. It is of significance for all organizations to have an effective response plan in place. Companies who are unprepared with a proper response plan will not be ready when an incident occurs.

RESPONSE STEPS

1. Resolve the problem
2. Identify what has been lost and who has been impacted
3. Continue operations while problems are being fixed
4. Communicate with stakeholders
5. Comply with applicable laws and reporting
6. Report to appropriate agencies

First, a special team should be established to handle and respond efficiently and effectively. The team should include technical support professionals; someone who can make financial and strategic decisions, such as a CEO and CFO; as well as operations executives, such as representatives from corporate communications and audit and compliance. In other words, key personnel who are responsible for implementing and monitoring the action plan should be integrated and kept informed of the plan. The legal team will also help shape the response plan, minimize the legal risk and advise how best to communicate with affected individuals, media and other third parties. Certainly, a team leader is important as well to ensure all the response actions are implemented properly.

Second, before the incident occurs, a risk management framework should be designed, including response protocol based on different incident types according to its influence and urgency. This framework should include the preparation, incident identification and assessment, communication, influence control and eradication, recovery plan and post-incident practice. Any third party that will assist, such as privacy counsel and cybersecurity professionals, should also be determined and stated explicitly in the plan.

Once there is a breach, the security response team members should be assembled and begin the investigation. Identify the problem and develop an effective action plan referring to the existing risk management framework. Fix the issue first, and then evaluate the extent of the attack and the scope of the incident. All information related to the incident should be collected including device, hardware and database activities, in order to further investigate and determine any legal liability and revise the protocol to comply. During the investigation, internal and external communications cannot be avoided. A statement should be prepared for public communication and interaction with the media. Finally, ensure the threat caused by the incident is eradicated, keep records and recover the business operation.

Step 5. Recover

When a company enters the recovery stage, it is past the immediate need to handle the cyber event and is now focused on the full restoration of normal systems and operations. During this stage, ongoing efforts are continued to mitigate the cyber event, but focus is also turned to the future and continuous improvement over time. At this point, a company should analyze its systems, policies and controls in place to determine if changes need to be made.

By following these five steps, businesses will be better prepared to face off with cybercriminals and prevent data loss. The hospitality business is connected to its guests in a myriad of ways… hotel guest data, spa health data, private club member data, restaurant guest data and employee data. The key to collecting data is to collect only the information of utmost importance for your business and to purge the ancillary information. Secondly, safeguard the data your business retains to ensure that cybercriminals cannot access the data and destroy the confidence of your guests.

CYBER INSURANCE | What is Covered

Cyber insurance is gaining in popularity as the incident of cybercrimes has grown, along with new laws and regulations which will increase the costs associated with a data breach. Insurance companies will look at multiple areas when assessing a client's risk for cyber insurance purposes.

Areas Reviewed in a Risk Assessment

- Dedicated resources
- Policies and procedures
- Employee awareness
- Incident response
- Security measures
- Vendor management
- Board oversight

Common Cybersecurity Coverage:

- Data breach
- Business interruption
- Privacy liability
- Electronic media liability
- Digital asset disruption
- Intellectual property
- Reputational harms
- Forensics
- Fraud
- Legal costs
- Public relations
- Data leakage

Remember policies are not a one-size-fits all, and a company's unique risks and exposures are to be considered when developing a policy.

DATA PROTECTION

What Part Do Data Protection Laws and Regulations Play In The Process?

Governments around the world are setting regulations pertaining to data protection and security, and systems for protecting that data are now a business reality and best practice. The headline-grabbing regulation is the European Union's General Data Protection Regulation (GDPR), which will be effective on May 25, 2018. It is the most stringent law to date when it comes to the treatment of personal data. But other countries are sure to follow suit or have already implemented their own, including Canada, China, Singapore and South Korea.

Data protection is nothing new to the hospitality industry, yet GDPR has made it more relevant and noteworthy than ever. Companies need to be aware of the regulations in the countries where they conduct business and know how these rules will impact their businesses.

In the case of the GDPR, the impact will not only be felt throughout the EU, but this regulation also applies to companies operating outside of the EU who handle the personal data of individuals from the European Union. What is causing businesses to take notice is that noncompliance results in a big bite for those in violation, in both huge fines and legal backing. There are two levels of fines: the first is up to €10 million or 2 percent of a company's global annual turnover of the previous financial year, whichever is higher; and the second is up to €20 million or 4 percent of a company's global annual turnover of the previous financial year, whichever is higher. The regulatory fines are viewed on a per case basis and are based on criteria such as the intentional nature of the infringement, how many people are impacted by the violation and whether the enterprise has had previous violations.

COMPLIANCE TEAM

A CROSS-DEPARTMENTAL TEAM SHOULD DEVELOP THE COMPLIANCE STRATEGY

" It is important to create a cross-functional dialogue and break down the silos between the various departments when planning for the impact of new regulations such as the GDPR. Cybersecurity and data protection planning should involve, at a minimum, representatives from the following areas: information technology, human resources, legal and compliance, security and risk. All of these need to be involved in developing an ecosystem to support the effort involved in implementing new processes to conform to legal requirements."

Stephen Barth

Founder, HospitalityLawyer.com

Consulting firm PWC indicated that the majority of U.S. companies doing business in Europe (68 percent) are planning to spend between US$1 million and US$10 million on upgrades to comply with GDPR. Gartner estimates that worldwide spending related to securing technologies will jump from US$86 billion in 2016 to US$108 billion in 2030.

Getting Ready for Data Regulation

All organizations should consult legal counsel while developing a data protection plan to determine their legal and reporting requirements pertaining to cybersecurity breaches and data losses. Countries around the world have varying levels of data security legal requirements and reporting. It is imperative to look at where customers

HOSPITALITY GDPR RESOURCES

As hospitality companies prepare to make operational changes to conform with the EU General Data Protection Regulation (GDPR), The HFTP GDPR/HDPO Task Force has prepared resources for the industry. Reference these guidelines as your company fits its security operations to comply with regulations.

- **Vendor Compliance Query Template** *(English, French, Spanish and German)*
- **Hospitality Data Protection Officer Job Description**
- **Hospitality Organization Data Flow Charts**
- **Privacy Policy Guidelines**
- **Registration Card** *(guest consent management guidelines)*

Locate these resources at ***www.hftp.org****.*

DATA PROTECTION

are located, where data is stored, third-party vendors and where the organization operates before finalizing a plan. Since the hospitality environment is unique in its infrastructure, prioritize using an industry specialist. Someone who understands the flow of guest data and how it is typically used, this will go a long way in uncovering the web of data accumulated by hospitality companies.

It is also imperative to review all contracts with vendors who have any touchpoints with data that contains PII or payment information. Start a conversation with third-party vendors expressing your intent to comply with the regulations and ask that the company participate in an assessment of data security and privacy measures, from the technical to the procedural. Request the vendor's compliance timetable, a confirmation of where your data is stored and a schedule to make contract adjustments reflecting regulation requirements.

With the new regulations, it is crucial to delineate in contracts and service agreements where the protection responsibilities lie in differing scenarios. Depending on the ownership structure — independent hotel, branded hotel, etc. — this includes vendor agreements, management contracts and franchise agreements.

The determination of the controller vs. the processor is important. As defined by the regulation, the controller is the entity that determines the purpose and use of the data, while the processor processes the data on behalf of the controller. Multiple purposes can present themselves for data use in the lifespan of collected data and it is not always clear which party is the controller and which is the processor in each scenario. When reworking agreements, define which is which and explicitly state it in the wording. This helps each party know its data management responsibilities.

Payment Information Security

In addition to legal considerations, hospitality and tourism organizations must also comply with standards such as the Payment Card Industry Data Security Standard (PCI DSS). PCI DSS, first released in 2004, was developed to enhance cardholder security and applies globally to all entities involved in payment card processing such as merchants, processors, acquirers, issuers and service providers. The basic requirements and security assessment consist of six major areas: building a secure network and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, monitoring and testing networks, and maintaining an information security policy.

Data processing systems must be configured in a way to allow organizations to properly secure data to comply with data security standards. Unfortunately, many systems were not architected in a way to facilitate this process. For example, most organizations use a payment card processor who provides an encrypted reference, token, to the hospitality organization to facilitate the payment process and remove the need of storing payment card information at the property. Up until recently, hospitality organizations have been at the mercy of software system suppliers who have only recently begun

PCI DSS 12 Step Checklist

REQUIREMENTS AND SECURITY ASSESSMENT PROCEDURES

- **Build and Maintain a Secure Network and Systems**
  1. Install and maintain a firewall configuration to protect cardholder data
  2. Do not use vendor-supplied defaults for system passwords and other security parameters
- **Protect Cardholder Data**
  3. Protect stored cardholder data
  4. Encrypt transmission of cardholder data across open, public networks
- **Maintain a Vulnerability Management Program**
  5. Protect all systems against malware and regularly update anti-virus software or programs
  6. Develop and maintain secure systems and applications
- **Implement Strong Access Control Measures**
  7. Restrict access to cardholder data by business need to know
  8. Identify and authenticate access to system components
  9. Restrict physical access to cardholder data
- **Regularly Monitor and Test Networks**
  10. Track and monitor all access to network resources and cardholder data
  11. Regularly test security systems and processes
- **Maintain an Information Security Policy**
  12. Maintain a policy that addresses information security for all personnel

Source: pcisecuritystandards.org

adding tokenization to their systems. When purchasing new systems, hospitality owners and operators must specify the latest security features to be incorporated in software systems and technologies to safeguard valuable data. The upfront cost may be expensive, but organizations will ultimately save money by safeguarding data. Organizations who experience a data breach face multiple costly consequences such as compensation and remediation costs, legal action, bank fines, lost revenue, damaged reputation and federal audits.

How Can Businesses Mitigate Exposure?

Securing data must be a strategic process involving everyone within the organization. Your company's first step is to implement a cybersecurity management plan, with actions to prevent data loss and a continuity plan ready to go in the case of a breach. Your main defense will be to train staff on the security risks, how to minimize them and how to detect an infiltration. This is an ongoing process that needs continual maintenance: make sure software and systems are up-to-date, as well as firewalls and anti-virus programs. Also consider having a third-party review the plan to pinpoint weaknesses in the plan.

Specifically, when it comes to securing data, a cross-departmental team should be put in place to analyze systems and determine where data is being held. Only important data, essential to business operations, should be collected and retained to mitigate any exposure from possible data losses. In addition, this data must be collected and maintained in accordance to legal and industry standards, such as PCI DSS and GDPR. According to the *2017 Cost of Data Breach Study* published by IBM, the average per capita cost of a data breach in the hospitality industry was US$12,410. With data breaches involving thousands of pieces of data, the cost of a data breach can rise quickly into millions of U.S. dollars.

Hospitality and tourism organizations store copious amounts of data pertaining to their clientele and confidential company information which must be safeguarded. Whether it be credit card data, personal information, or confidential company files, all of this information must be protected. If a company is compromised and hackers gain access to this data, it would cause major detriment to the organization whether it be to its reputation, legal or financial standing. According to the *2018 Verizon Data Breach Investigations Report*, the accommodations industry reported 338 breaches in 2017 placing it in third place for the greatest number of data breaches reported. Beyond the imposed requirements, data management is a business reality and it is imperative as a hospitality company to take care of our guests as best we can — including doing our best to protect their data. Operators must take action and protect our guests and this valuable information. ■

SOURCES

1. *PCI Security Standards Council. (2017). Retrieved September 29. 2017 from https://www.pcisecuritystandards.org/.*
2. *World Tourism Organization. (2017). Retrieved September 29, 2017 from http://www2.unwto.org/.*
3. *Derousseau, R. (September 2017). A big payoff for cybercop stocks. Fortune, 176(3):19-21.*
4. *Newhouse, W. & Weeks, S. (2017). Securing property management systems: cybersecurity for the hospitality sector. Retrieved September 29, 2017 from https://csrc.nist.gov/publications/detail/white-paper/2017/04/28/[project-description]-securing-property-management-systems/draft.*
5. *Sullivan, P. (2017). What to do when cybersecurity breaches seem inevitable. Retrieved September 29, 2017 from searchsecurity.techtarget.com.*
6. *National Cyber Security Alliance. (2017). CyberSecure My Business. Retrieved September 29, 2017 from staysafeonline.org.*
7. *Verizon. (2018). 2018 Data breach investigations report retrieved April 10, 2018 from http://www.verizonenterprise.com/verizon-insights-lab/dbir/.*
8. *European Union Agency for Network and Information Security. (2016). Cyber insurance: recent advances, good practices and challenges. Retrieved October 2, 2017 from www.enisa.europa.eu.*
9. *IBM. (2017). Ponemon Institute's 2017 cost of data breach study: global overview. Retrieved October 2, 2017 from https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=SEL03130WWEN&.*

SECURITY BEST PRACTICES

Plan

Implement a cybersecurity management plan, including a continuity plan.

PREVENT DATA LOSS

- **Use Strong Passwords**: Use unique account names, complex passwords, change passwords on POS systems on a regular basis and deploy multi-factor authentication.
- **Restrict Access to the Internet**: Restrict access to POS system computers or restrict terminals to POS-related activities.
- **Disallow Remote Access**: Prevents unauthorized access, remote access to the POS network at all times should be limited.
- **Detect Insider Threats**: Insider threat is the most frequent and costly incident.

Update Software and Systems

Ensure that updated software systems are being used.

Install Firewalls, Use / Update Antivirus Programs

Use firewalls and regularly update antivirus programs to maintain effectiveness against newer versions of malware.

Train Employees

Train employees on information security and privacy awareness, including anti-phishing and social engineering exercises.

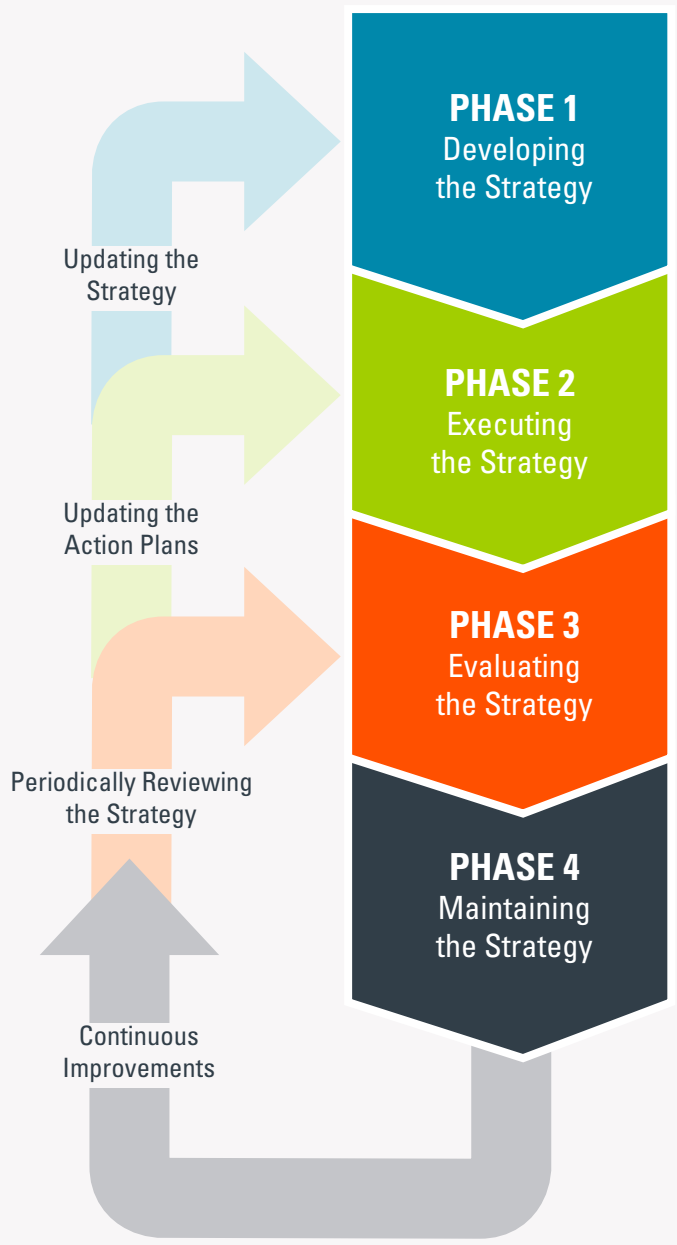
Incident Response Planning

Provide a framework to manage a cybersecurity incident.

Third-party Assessment

Obtain a third party assessment of your cybersecurity program and framework.

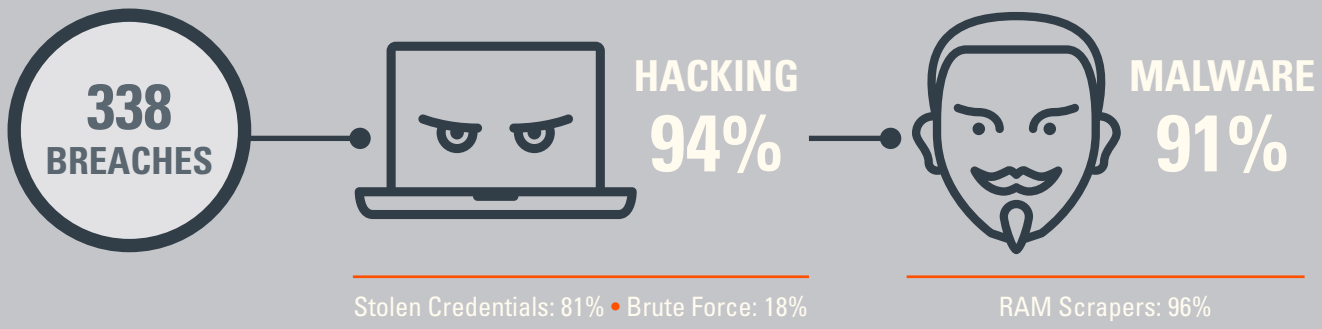
Cybersecurity Strategy Lifecycle



Source: National Cyber Security Strategy Lifecycle developed by the European Union Agency for Network and Information Security (2016)

DATA BREACH TYPES

TOP CYBER THREATS TO THE HOSPITALITY INDUSTRY



Source: Verizon 2018 Data Breach Investigations Report 11th Edition

MALWARE

Malware, short for malicious software, is an umbrella term used to refer to any harmful or intrusive software designed to cause damage to a single computer, server or computer network.[1] The top malware variety within hospitality industry breaches in 2017 was RAM scrapers (96%).

RAM Scraper

What is it? Short for random access memory scraper, this is a malware that scans the memory of digital devices and collects sensitive personal information. POS systems are notably targeted for the large amount of payment information processed daily.[3, 4]

How does it happen? The scraper software is usually disguised as something innocuous and gets introduced to the system in various ways, such as unpatched system vulnerabilities, a malicious e-mail attachment mistakenly opened by an employee or even a resentful employee.[4]

C2

What is it? Also known as C&C, short for command-and-control servers, these are used by attackers to communicate with compromised systems within a target network by issuing commands and controls. They can be used for malicious actions such as remote control or data exfiltration.

How does it happen? A commonly used method for a malware infection is through email phishing attempts.[5]

Spyware/Keylogger

What is it? A software that tracks and reveals every click, touch, download and conversation on a digital device.

How does it happen? Spyware can be installed on systems when an infected website is visited or when an infected file attachment of an e-mail, text message, P2P networks, instant message or social networks is opened.[6]

Backdoor

What is it? An application that allows for remote access to computers and networks. It can often help attackers break into the infrastructure without being discovered.

How does it happen? Backdoor attacks are conducted in the same manner as spyware and keylogging attacks, via infected websites and file attachments.[7]

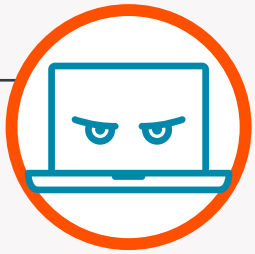
Export Data

What is it? Many applications support downloading data as a CSV file. Such data are often user controlled data, which can be injected for malicious purposes such as running system level commands and stealing information.

How does it happen? An application usually cannot control what a user enters, thus a malicious formula could be inserted and executed when the exported file is opened.[8]

DATA BREACH TYPES

HACKING



Hacking is an unauthorized intrusion into a computer or a network. Hackers alter systems or security features to accomplish a goal that differs from the original purpose of the system.[9]

Hacking can happen when a highly-skilled computer programmer discovers and takes advantages of an exploit or vulnerability in a computer system or network.[10] Hackers may use a variety of methods and tools. The following are the top ones used in hospitality industry breaches.

Use of Stolen Credentials

What is it? Hackers use credentials stolen by themselves or others to do the hacking. Credentials usually contain a person's personal information and/or access to systems and networks.[11]

Brute Force

What is it? Brute force, also known as brute force cracking, is a trial and error method used by application programs to decode encrypted data such as passwords through exhaustive effort. Although time-consuming, it is considered to be infallible in theory.[12]

How does it happen? Hackers may use widely available tools to launch brute force attacks. Such attacks are easy to detect, but not easy to prevent.[13]

Social

What is it? Social engineering, in the context of information security, typically refers to psychological manipulation of people into performing actions or divulging confidential or sensitive data.

How is it done? Social engineering commonly involves communication that invokes urgency, fear or similar emotions in the victim, leading the victim to promptly reveal sensitive information, click a malicious link or open a malicious file.[14]

Use of Backdoor/C2

What is it? As mentioned previously, backdoor and C2 are commonly used types of malware. Hacking can be done by employing these techniques.

Phishing

What is it? Phishing is the attempt to obtain sensitive information, often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.[15]

How does it happen? Malware attacks, especially via a malicious e-mail attachment or an e-mail with an embedded malicious link. Phishing can also be done via phishing websites, social media attacks, spear-phishing, fraudulent tax returns, phishy phone calls, charity phishing and CEO phishing.[16]

Misuse

Privilege misuse can cause data breaches when users with privileged accounts mishandle the data or maliciously compromise the data and system. Typical users of privileged accounts include system administrators, network engineers, database administrators, data center operators, upper management and security personnel.[16]

1. *https://technet.microsoft.com/en-us/library/dd632948.aspx*
2. *Verizon 2017 Data Breach Investigations Report 10th Edition*
3. *http://searchsecurity.techtarget.com/definition/memory-scraping-malware*
4. *https://www.recode.net/2014/1/13/11622240/what-the-heck-is-a-ram-scraper*
5. *http://searchsecurity.techtarget.com/feature/Command-and-control-servers-The-puppet-masters-that-govern-malware*
6. *https://securingtomorrow.mcafee.com/consumer/family-safety/what-is-a-keylogger/*
7. *https://blog.trendmicro.com/backdoor-attacks-work-protect/*
8. *http://www.tothenew.com/blog/csv-injection/*
9. *https://www.techopedia.com/definition/26361/hacking*
10. *https://www.echosec.net/what-is-hacking-how-does-it-work/*
11. *https://www.secplicity.org/2017/05/18/stolen-hackers-data/*
12. *http://searchsecurity.techtarget.com/definition/brute-force-cracking*
13. *https://www.owasp.org/index.php/Blocking_Brute_Force_Attacks*
14. *https://digitalguardian.com/blog/social-engineering-attacks-common-techniques-how-prevent-attack*
15. *https://en.wikipedia.org/wiki/Phishing#cite_note-1*
16. *http://blog.cybertraining365.com/2017/03/24/big-cyber-threats-break-down-types-cyber-attacks/*
17. *https://www.scmagazineuk.com/the-threat-of-privileged-user-access--monitoring-and-controlling-privilege-users/article/568624/*

ABOUT HFTP

Hospitality Financial and Technology Professionals (HFTP®) established in 1952, is an international, nonprofit association, headquartered in Austin, Texas, USA, with offices in Hong Kong, United Kingdom, the Netherlands and Dubai. HFTP is recognized as the spokes group for the finance and technology segments of the hospitality industry with members and stakeholders spanning across the globe. HFTP uniquely understands the industry's pressing issues and assists its stakeholders in finding solutions to their challenges more efficiently than any organization. It does this via its expert networks, research, certification programs, information resources and conferences/events such as HITEC. HFTP also owns the world's only hospitality-specific search engine, PineappleSearch.com. For more information about HFTP, e-mail membership@hftp.org. Read industry updates on the suite of HFTP hospitality news sites: HITEC Bytes, Club Bytes, Finance Bytes, GDPR Bytes and HFTP News.

2017–2018 HFTP GLOBAL BOARD

EXECUTIVE COMMITTEE

PRESIDENT
Timothy G. Nauss, CHAE
CFO
Macao Studio City

VICE PRESIDENT
Scot Campbell, CHTP
CTO
North American Concerts, Live Nation

TREASURER
Michael Levie, CHTP
COO
citizenM Hotels

SECRETARY
Mark Pate Sr., CHAE, CHTP, MBA
Assistant Controller and IT Director
Highpointe Hotel Corporation

IMMEDIATE PAST PRESIDENT
Lyle Worthington, CHTP
CIO
The Student Hotel

EXECUTIVE ADVISOR
Jill Burnett, CHAE, CPA
Controller
Medalist Golf Club

DIRECTORS

Stephanie Anderson, CHAE, CPA, CGMA
CFO
River Bend Golf & Country Club

Cindy Braak
SVP, Finance Business Partner
Marriottt International Inc.

Cindy Estis Green
Co-founder & CEO
Kalibri Labs, LLC.

Md Amirul Islam
Assistant Manager, Income Audit
Marriott Autograph Collection

Sherry Marek
Co-founder and Vice President
Datavision Technologies, Inc.

Martha Mazzitelli, CAM, CHAE+, CHTP+
CFO
Bay Colony Shared Services

Nick Price
CEO
Netsys Limited Technology

Laurie Rozeski, CHAE, MBA
CFO
Wildcat Run Golf & Country Club

Kaeko Shirasu-Bailey, CPA
Assurance Senior Manager
RSM US LLP

Justin Taillon, MBA, Ph.D.
Professor & Department Head
Highline College

Derek Wood
Managing Director
Derek Wood Associates Ltd.

Ex Officio
Frank I. Wolfe
CEO
Hospitality Financial and Technology Professionals (HFTP)

CHTP
CERTIFIED HOSPITALITY TECHNOLOGY PROFESSIONAL

Set yourself on a PATH OF PROFESSIONAL EXCELLENCE with these hospitality specific designations.

CHAE
CERTIFIED HOSPITALITY ACCOUNTANT EXECUTIVE

A service of Hospitality Financial and Technology Professionals (HFTP®)

TAKE THE NEXT STEP IN YOUR CAREER

As a committed hospitality finance or technology professional, you want to take the next step in your career. Elevate your professionalism and demonstrate your industry expertise with HFTP's Certified Hospitality Accountant Executive (CHAE®) and Certified Hospitality Technology Professional (CHTP®) designations.

HFTP's certification programs are globally recognized for setting industry standards for hospitality finance and technology. The CHAE and CHTP certifications are the only certifications offered by HFTP which are specific to the hospitality industry.

Earning Your Designation
To earn the designation, you must pass the designation exam. Get started by completing the application process and include the required materials needed to take the exam.

Exam Preparation
HFTP offers individuals resources to prepare for the exam, such as the practice exam and review sessions, both available online and at HFTP events.

Renew and Be Active
Once you achieve your designation, stay active by earning continuing education points over the course of two years to renew your certification. HFTP offers continuing education at all its conferences and events, as well as at HFTP chapter events and HFTP online education.

Start Investing in Yourself Today

Take the first step in your professional development and e-mail **certification@hftp.org** or visit **www.hftp.org/certification** for information about the HFTP CHAE and CHTP designations.