Risk Assessment Analysis for VB Tiki Tours

Team VB Tiki Tours

COVA CCI sponsored ODU Cybersecurity Clinic

Spring 2026 Semester

Team Members: Hans Peterson, Marquais Hendrick, Tyler Royster

CYSE 368: Cybersecurity Internship

4/23/2026

Table of Contents

Introduction

Our Team

Our purpose, as the Cyber Clinic, is to provide Cybersecurity-as-a-Service to various micro and small businesses in Hampton Roads through a free risk assessment. The goal of the assessment is to raise overall cybersecurity awareness by providing best practices on various topics such as risk management, network defense, policies, procedures, and employee training, while considering the needs of the small businesses.

Team Members:

Marquais Hendrick

I scheduled group meetings outside of class time and acted as the main communicator with Mr. Hegrenes. In the sections of the report, I completed the risk assessments for the CISA CPG 2.0 and SWOT analysis, and I assisted with the NIST risk assessment by researching solutions to the six Functions. Additionally, I interviewed Mr. Hegrenes for Valor's Top 10 Digital Security Checklist.

Hans Peterson

I formulated interview questions for Mr. Hegrenes, defined the scope of VB Tiki Tours' needs, organized ideas and documents, assisted with drafting the risk assessment analysis report, reviewed the team's findings, and spearheaded the research focus towards Mr. Hegrenes' goals. In the sections of the report, I completed the introduction, including company information, and I assisted with researching/completing the NIST risk assessment and Valor's risk assessment.

Tyler Royster

I kept steady contact with the CEO, Tory Hegrenes. I acted as a reliable standby in case neither team member could meet with Mr. Hegrenes, sent follow-up emails, scheduled the location for the team to meet, and created templates for the team to follow regarding the report and presentation. On the sections of the report, I handled the overall formatting, completed the Next Steps section, and organized our APA references.

Overview of the Hospitality Industry

The hospitality industry is a widely encompassing sector that includes businesses such as hotels, bars, theme parks, travel agencies, and tourism. The primary purpose of the hospitality industry is to "deliver comfort, convenience, and positive guest experiences rather than essential goods" (Agarwal, 2026). Rather than producing necessities, the industry focuses on aspects such as leisure and entertainment. Though the industry may be perceived as "unnecessary," it is pivotal to the development of the global economy and job creation. For tourists, first impressions matter, which is what the hospitality industry aims to excel in.

Notably, the travel and tourism sector in the U.S. in 2024 contributed nearly 2.6 trillion U.S. dollars to the nation (Statista Research Department, 2026). Additionally, there were nearly 2.4 billion leisure and business domestic trips in the U.S. in 2025 (Statista Research Department, 2026). The tourism sector is one of the strongest drivers of the hospitality industry; it is also the sector that VB Tiki Tours specializes in. Why then is the growth of the hospitality industry so important? Where there is profit, there is crime. Where there is technology, there are cyberthreats.

Threats Associated With the Hospitality Industry

Due to an influx of technology and sensitive data, the most common threats the hospitality industry currently faces are phishing, ransomware, and denial of service attacks (Marino, 2025). These threats seek to exploit weak security measures, such as the lack of strong employee passwords, user awareness, system updates, and even network monitoring tools. The worst attacks are ones that maintain secrecy; to the victim, it would appear as if no attack occurred at all. Therefore, it is best to assume that attacks are a certainty, not a possibility. It is a matter of when, not if.

One of the most common and simplest threats that businesses within the hospitality industry face is phishing attacks. Phishing is a method of social engineering that involves an adversary crafting a message to gain access to a target's systems (Itkin et al., 2025). An alternative focus of phishing is to gain sensitive information from a target. Either way, the intent is to trick a target into providing unauthorized access. In a phishing attack, the adversary sends a specially crafted email to the victim, and this email may contain attachments designed to execute malicious code. However, adversaries may use other means, such as social media platforms, to reach a target. Adversaries may also pretend to be a trusted source or request a target to contact them through a phone number to receive instructions on downloading malware (Itkin et al., 2025). Phishing is a prevalent threat, and it will not disappear in the near future. The simplest, cost-efficient ways to prevent or mitigate phishing attacks is by raising employee cybersecurity awareness; phishing emails normally have grammatical errors in the header and content, and have suspicious requests to access links. If an offer seems too good to be true, then it is best to assume that it is a lie. Ultimately, it takes experience to distinguish phishing emails from genuine ones.

Another common threat to the hospitality industry is ransomware. According to the Internet Crime Complaint Center (IC3) (2023), ransomware is a type of malware that prohibits a user from accessing their files, system, or networks until a certain demand is met, commonly in the form of paying a ransom. Ransomware can easily disrupt operations and result in the loss of critical systems and data. They can be unknowingly downloaded from an email attachment, accessing a link, or even visiting an infected website, and once the ransomware is loaded, it will lock access to affected devices (Internet Crime Complaint Center (IC3), 2023). There have been several widespread ransomware attacks in the past, and they will persist in the future.

One last common threat to the hospitality industry is denial-of-service attacks. MITRE distinguishes two types of Denial of Service attacks: Endpoint Denial of Service and Network Denial of Service. However, the most common form is the endpoint version. In an endpoint denial-of-service attack, an adversary attempts to “degrade or block the availability of services to users” (Oliveira et al., 2025). Essentially, a system or website’s services are exhausted to the point that it is unable to provide service to actual users; adversaries use methods, such as botnets, or networks of infected devices, to access the website. With enough infected users on the website, the system will halt, thus preventing real customers from using the website.

Company Information

Company Description

VB Tiki Tours is a small tourism business that provides Tiki-themed boat tours on the waters of Virginia Beach. The cruises on the Lynnhaven River Basin and Broad Bay waterways last a leisurely one hour and fifty minutes, and these tours are conducted all year round. Guests, such as friends, family, and colleagues may provide their own set of food and beverages on these tours. Up to six guests can board the Tiki-themed boat, Rum Shaker, with prices of approximately $60 per person. On board, one of four USCG certified Master Captains of VB Tiki Tours will tour the guests over the waterways.

Company History

After spending time in Key West, Florida, and seeing tiki boats, Tory Hegrenes brainstormed a tiki-themed business of his own, which is now known as VB Tiki Tours. In 2023, VB Tiki Tours opened its tourism services to the public and received attention on 13News Now. The tiki boat, known as the Rum Shaker, was used to tour customers at Long Bay Point. Three captains, Ben, Ron, and Taylor, assisted with touring the Rum Shaker over the waters. Additionally, yoga instructor Jennifer Wolfe joined the VB Tiki Tours team. After two years, VB Tiki Tours entered its 4th season, and the Rum Shaker was replaced and upgraded by the Rum Shaker II.

Company Social Media Presence

VB Tiki Tours has four social media accounts; they have an X (formerly Twitter), Instagram, Facebook, and Threads account. They are active on their Instagram, Facebook, and Threads accounts, with the most recent posts being published mere days ago. However, their X account is post protected, and without following the account, its activeness is unverifiable; assuming it is inactive, it would be best to delete or de-activate the account to prevent any potential unauthorized logins to the account. There are 2,310 followers and 188 posts on Instagram, 2,100 followers on Facebook, and 245 followers on Threads. There are no dedicated personnel that manages the social media accounts, so Mr. Hegrenes (owner) is responsible for controlling all four accounts. VB Tiki Tours frequently reports updates to their business, such as the removal of the Rum Shaker on February 18, 2026, and the participation as a “Shark” for ODU’s entrepreneurial class on the week of December 6, 2025. In general, VB Tiki Tours has a very active social media presence and is popular.

Risk Assessments

Valor's Top 10 Digital Security Checklist

For the VB Tiki Tours Risk Management Report, we were able to work with Valor Cybersecurity as a trusted partner to the Cybersecurity Clinic. Valor Cybersecurity (CEO Greg Tomchick) is a small business owner who provides scalable, adaptive cybersecurity protocols to other business owners. Based on our clinic meetings with Greg, this is our suggested write-up based on the Valor Cybersecurity Digital Checklist Assessment. Valor's Top 10 Digital Security Checklist provides both an overview of the business's strengths and weaknesses. There are a total of 10 questions, with each question having a maximum score of 5 and a minimum score of 0. VB Tiki Tours scored 27 out of 50, placing it in the moderate risk category. There are many objectives within Valor's Digital Security Checklist that VB Tiki Tours scored well in, but there were also several concerning weaknesses. This assessment will run through the checklist from VB Tiki Tour's most successful objectives to its least successful.

Annual Digital Risk Checkup

In terms of risk assessments, VB Tiki Tours scored 5 out of 5. It was evident that VB Tiki Tours had a good understanding of the risks posed to their people (e.g., employees, customers) and assets.

Access Check and Minimal Permissions

In terms of access control, VB Tiki Tours scored 5 out of 5. They provided details of recent reviews of access to key systems, data, and information. This provided insight into the organization's ability to maintain appropriate levels of visibility and control over critical data and adherence to strong governance measures.

Digital Surveillance

In terms of digital surveillance, VB Tiki Tours scored 4 out of 5 as well. They had an excellent approach to surveillance and monitoring of activity, physical security measures, and detection of any unlawful access to their employees, customers, visitors, and premises. However, our team noted several moderate areas for improvement, such as the camera placement on the Rum Shaker II with a limited field of view; there are so-called blind spots within the current positions of the surveillance cameras. Moreover, the cameras' batteries must be manually replaced, and since employees of VB Tiki Tours are relatively preoccupied with the boating business, the cameras may run out of energy without anyone noticing.

Backup Data and Software, then Test

In terms of backup and recovery processes, VB Tiki Tours scored a 3 out of 5. Although backups are performed on a regular basis, the company is lacking in consistently testing those backups. Additionally, VB Tiki Tours does not adhere to the 3-2-1 rule for backups; there is only one backup copy containing all of VB Tiki Tours' data, and this copy is located on a cloud platform on Google Drive. There are two other backups on physical hard drives, though one contains the customer database and the other contains the employee database. As a result, the company is largely flying blind in its ability to recover from events like ransomware attacks should these backups be tampered with or destroyed. Having backups can hasten the recovery process and save thousands of dollars in daamge. The most important data to secure are customer reservations and payment information. Tour details, schedules, and employee data are also essential. The goal is to keep business running smoothly and maintain profitability should a disruption to operations, such as a ransomware attack, hardware failure, or unauthorized actions by individuals with access to its cloud-based data storage account, occur. Daily bookings could

not be honored, payments processed, or customer contacts made. Lost revenue and erosion of customer trust would quickly threaten the agency's bottom line and, in the long term, its very existence.

Having backups on hand means that if something were to go terribly wrong with your systems, you would be able to return to a prior point in time and more quickly get back to business as usual. However, having a backup is not simply having a file on a disk; it must be reliable, safely stored, and easily restorable. Having multiple copies of your data and storing those copies in physically separate locations is typically the best method, and you should actually practice recovering your data from time to time to ensure that the process is possible when needed most. This is especially important for tour operators such as VB Tiki Tours, who run the risk of being the target of ransomware, in addition to less severe issues with human error and intermittent system failures. Protecting your data and systems from these events actually reduces your loss should something occur. By treating your backup strategy seriously, you can turn a worst-case scenario into business as usual.

Digital Personnel Management

In terms of VB Tiki Tours onboarding and offboarding processes, VB Tiki Tours scored a 3 out of 5. While the company has a number of processes in place, they are not always fully implemented or kept current, which can put employees and clients at risk of social engineering tactics or permit excess access to linger in the company's systems. While the business scored well when it came to the key issues most critical to its operation, there were some more secondary issues where it scored equal to or less than 2 out of 5. For the areas where VB Tiki Tours scored 2 out of 5, there are several clear opportunities for improvement that would significantly strengthen the company's overall security posture. First, the organization should

implement multi-factor authentication (MFA) across all critical systems, including email, cloud storage, and any administrative accounts, to reduce the risk of unauthorized access from compromised credentials. Second, deploying a properly configured network firewall would help prevent unauthorized external access and provide a layer of defense against common network-based attacks. Third, the company should develop and maintain a formal incident response plan, outlining clear procedures, roles, and communication steps to follow in the event of a cybersecurity incident, which would minimize confusion and reduce response time. Additionally, implementing regular system monitoring and logging would improve visibility into suspicious activity and allow for quicker detection of potential threats. Finally, standardizing and enforcing security policies and procedures, including periodic reviews and updates, would ensure consistency across the organization and reduce gaps caused by informal or outdated practices. Together, these improvements would address key weaknesses, reduce overall risk exposure, and enhance the company's ability to prevent, detect, and respond to security threats effectively.

Employee Bootcamp

In terms of cybersecurity awareness training, VB Tiki Tours scored a 2 out of 5. After the Google Business Review attack and the sudden phishing attack that sent out unauthorized emails to people connected to VB Tiki Tours' email address, there were talks regarding the incident. However, there was no establishment of an actual training program that assessed the employees' cybersecurity awareness. Implementing a structured cybersecurity awareness bootcamp would be highly beneficial for VB Tiki Tours because it transforms informal discussions into measurable, proactive defense against real threats. The recent phishing incident and Google Business Review attack show that employees are already being targeted, and without proper training, human error remains one of the company's biggest vulnerabilities. A bootcamp would provide hands-on,

scenario based learning such as identifying phishing emails, recognizing social engineering tactics, and responding appropriately to suspicious activity so employees are not just aware of threats but know exactly how to act in real time.

Double Layer Protection Shield

In terms of an added layer of security, VB Tiki Tours scored a 2 out of 5. While Multi-Factor Authentication (MFA) is used on some systems, it is not currently in use on critical ones, meaning there is potential for threat from compromised credentials. MFA is a security measure that requires users to verify their identity using two or more factors, typically something they know (e.g., password), something they have (e.g., phone or authentication app), or something they are (e.g., fingerprint or facial recognition). By requiring multiple forms of verification, MFA makes it much more difficult for attackers to gain access, even if they have obtained a user's password. Without MFA on critical systems such as email, cloud storage, or administrative accounts, VB Tiki Tours remains vulnerable to common attacks like phishing and credential stuffing. Implementing MFA across all essential platforms would significantly strengthen account security and reduce the likelihood of unauthorized access.

Digital Perimeter Guard

In terms of using a firewall, VB Tiki Tours scored a 1 out of 5. We understand that network firewalls are not in place on the external-facing network segments. The lack of a network firewall exposes your assets (e.g., databases) to external threats as well as potential malicious internal traffic. Therefore, we highly encourage the implementation of a firewall. Additionally, Virtual Private Networks (VPNs) can temporarily serve as a replacement for the lack of firewalls; in conjunction with active firewalls, they add a layer of security. A free VPN you may want to consider is Proton VPN.

Draft a Digital Playbook

In terms of establishing and maintaining a cybersecurity incident response plan, VB Tiki Tours scored a 1 out of 5. There is no formal incident response or information security policy in place. This means should a cybersecurity incident occur, there would be little knowledge or process in place to respond with, potentially leading to prolonged downtime and data loss. Development and implementation of a formal incident response plan, as well as regular testing of that plan, would enhance the organization's ability to respond to security incidents in a timely and effective manner.

Fortify Your Digital Mailbox

In terms of maintaining a secure email system, VB Tiki Tours scored a 1 out of 5. The lack of robust security mechanisms/settings in their email resulted in the infamous phishing attack. Fortifying your digital mailbox with a secure email system will be a large deterrence to phishing attacks. Because VB Tiki Tours scored a 1 out of 5 in securing its email system—and has already experienced multiple phishing incidents—this is a high-priority area that requires immediate remediation. Strengthening email security will significantly reduce the risk of future attacks, account compromise, and reputational damage.

One of the most critical improvements is implementing Multi-Factor Authentication (MFA) across all email accounts, especially administrative and shared inboxes. This ensures that even if credentials are stolen, attackers cannot easily gain access. In addition, the company should configure core email authentication protocols such as SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance). These help verify that emails sent from the company's domain are

legitimate and prevent attackers from spoofing the business's email address—one of the likely causes of the previous phishing incident.

VB Tiki Tours should also invest in advanced email filtering and threat protection tools, which can automatically detect and block phishing emails, malicious links, and suspicious attachments before they reach employees' inboxes. Pairing this with user-level controls, such as disabling automatic email forwarding and limiting external sharing, further reduces exposure. Another key remediation is implementing a formal cybersecurity awareness training program, including phishing simulations. Since employees are often the first line of defense, training them to recognize suspicious emails and report them quickly can drastically reduce successful attacks. Establishing a clear reporting process (e.g., a "report phishing" button or internal contact) ensures threats are addressed immediately.

Finally, the company should enforce strong password policies and consider using a password manager to prevent weak or reused credentials. Regular audits of email account activity and access logs should also be conducted to identify unusual behavior early. By implementing these controls, VB Tiki Tours can move from a reactive position to responding to attacks after they occur to a proactive security posture that prevents, detects, and mitigates email-based threats effectively.

NIST Assets, Risks, and Controls

What exactly is NIST? NIST is an acronym for the National Institute of Standards and Technology, and this agency was established by Congress in 1901 to remove major challenges to industrial competitiveness within the U.S. at the time (National Institute of Standards and Technology, 2022). Its vision, mission, and specialization has evolved over time, and they now focus on "the smallest of technologies to the largest and most complex of human-made creations" (National Institute of Standards and Technology, 2022). In essence, NIST is a pioneer in promoting innovation, competition, and equitable standards in technology solutions. NIST upholds certain values, such as perseverance, integrity, inclusivity, and excellence, which are present in their NIST Cybersecurity Framework.

What is the NIST Cybersecurity Framework? Currently on the 2.0 version, the NIST Cybersecurity Framework (CSF) is a document that provides guidelines for industries, government agencies, organizations, and other types of businesses to manage cybersecurity risks (NIST, 2024). These guidelines offer high-level overviews of cybersecurity outcomes that are flexible in nature; organizations, regardless of size and sector (e.g., public, private) can use the CSF 2.0 to better "understand, assess, prioritize, and communicate its cybersecurity efforts" (NIST, 2024). However, how these cybersecurity outcomes should be achieved is based upon an organization's discretion. No one size fits all. The same applies for cybersecurity solutions. An organization must consider its resources, goals, interests, and stakeholders before executing any one solution. Additionally, an organization must continually assess their cybersecurity posture all year round, as certain weaknesses may manifest over time. It is recommended that the following outcomes listed in the functions of the CSF Core are fulfilled, but they are not mandatory.

There are six functions of the CSF Core:

1. Govern (GV)
2. Identity (ID)
3. Protect (PR)
4. Detect (DE)
5. Respond (RS)
6. Recover (RC)

Govern (GV) Function

The first and broadest function is Govern (GV). This function involves an organization's cybersecurity risk management strategy, expectations, and policies, including how they are communicated and monitored (NIST, 2024). Governance, depending on the organization's goals, mainly informs how an organization should conduct itself to achieve the outcomes of the other five CSF Core functions. Good governance would include an establishment of cybersecurity risk strategies (e.g., supply chain), distinguished employee roles, and clearly defined responsibilities. Ultimately, governance is concerned with how an organization approaches a certain cybersecurity strategy; this way, the outcomes do not stray far from the mission.

We identified strengths and weaknesses in how VB Tiki Tours handles the Govern function. One of these strengths is the knowledge of regulatory requirements, such as boat insurance, a state boating license, and a captain's license (issued by the United States Coast Guard). However, in regards to an understanding of the legal, regulatory, and contractual requirements in cybersecurity, such as privacy and civil liberties, it is moderate. An additional strength of VB Tiki Tours is that there are risk management plans, including implementing cost benefit analysis. One potential weakness is that, in regard to the risk management plan, there is a non-formal method of tracking risk tolerance. It is more so a mental process of calculating risk

tolerance. These strengths and weaknesses were assessed using the **Organizational Context** and **Risk Management Strategy** categories under the Govern function of the NIST Cybersecurity Framework.

What are the recommendations for improving VB Tiki Tours' Govern Function?

Considering VB Tiki Tours' tight budget, it is highly recommended for the acting cybersecurity leader to research federal and Virginia's data privacy laws since the legal costs from infractions of these laws can be costly; as an example, there is the Virginia Consumer Data Protection Act (VDCPA), which gives Virginia residents certain rights over the personal data that businesses collect (*Code of Virginia Code - Chapter 53. Consumer Data Protection Act*, 2023). There is also the Virginia Personal Data Breach Notification Law (VPDBNL), Health Insurance Portability and Accountability Act (HIPAA), and Federal Trade Commission Act (FTCA). Additionally, it would be preferable if risk tolerance were written down on a document (i.e., risk management plan), as it maintains order/organization, can be quickly referred to should the need arise, and can be shared with internal stakeholders (e.g., employees). It is crucial for all internal stakeholders to be on the same page, as their actions should align with the risk management plan. Lastly, VB Tiki Tours can reassess their cybersecurity posture on a periodic basis (e.g., bi-monthly), so it is recommended to review the categories under the Govern Function; this applies to every other subsequent function.

Identify (ID) Function

The second function is Identify (ID). The Identify function is concerned with how the "current cybersecurity risks are understood" (NIST, 2024). To properly understand cybersecurity risks, an organization must take into account its assets (e.g., systems, hardware, software, data), including the services of third-parties and suppliers. Why exactly must an organization keep

inventory? Cyberthreats are opportunistic, and the most valuable targets are by far the weakest and easiest-to-exploit. Though the motivation of attackers/cyberthreats varies, they are selective in what they target. Additionally, the Identify function also includes identification of improvements for an organization's policies, plans, and practices to better support overall cybersecurity risk management (NIST, 2024).

We identified strengths and weaknesses in how VB Tiki Tours handles the Identify function. One of these strengths is an inventory of physical and virtual assets; for a year and a half, each asset was manually typed into a document. Additionally, the prices of each asset were tracked. Another strength is that the protection of these assets is based on prioritization (e.g., higher budget). However, one weakness is that the services of a third party, Fareharbor, used for online booking were not kept in an inventory. Lastly, there is a lack of updated cyber threat intelligence from information-sharing forums. These strengths and weaknesses were assessed using the **Asset Management and Risk Assessment** categories under the Identify function of the NIST Cybersecurity Framework.

What are the recommendations for improving VB Tiki Tours' Identify Function?

First, any services of a third party, such as Fareharbor, should be inventoried in a separate document. Third parties are a large risk since a business (i.e., VB Tiki Tour) cannot manage how a third party manages their cybersecurity (e.g., lack of MFA). A chain is only as strong as its weakest link. Sometimes, the third party or supplier is the weakest link, and these result in a broad attack on a supply chain. If a cybersecurity incident were to occur, third parties could be easily identified, including what services or data have been compromised or impacted. Additionally, there should be a source of cyber threat intelligence to stay up-to-date on cyberattacks. Knowledge is key to defense. Bearing these threats in mind, we pre-emptively

search for signs of these threats. We are more alert. It is not recommended to pore over every article, but a minute of reading should suffice. A few free recommended websites for cybersecurity news are The Hacker News, Reuters Cybersecurity, and Cyber Security News.

Protect (PR) Function

The third function is Protect (PR). The Protect function is the bulk or spearhead of how an organization will defend itself. This function is concerned with the "safeguards to manage the organization's cybersecurity risks," whether that be preventing, mitigating, transferring, or accepting a threat. This function, additionally, is massively supported by the Identify function since identifying assets also means identifying potential threats and solutions to counter said threats. Protect outcomes modify the likelihood and impact of adverse events (i.e., threats) and positive opportunities. A few outcomes under this function include employee training and awareness, access control, authentication, data security, and identity management (NIST, 2024).

We identified strengths and weaknesses in how VB Tiki Tours handles the Identify function. In terms of strengths, there are physical security mechanisms at VB Tiki Tours' workplace that protect unauthorized access to critical assets. For example, on VB Tiki Tours' boat, the Rum Shaker II, there are locks, two video cameras (one with night vision, both equipped with motion sensors), and the video data of these cameras are stored for ninety days. Additionally, VB Tiki Tours employees, namely the captains, only have access to what is sent to their personal email. Moreover, there are weaknesses. There is a lack of formal methods of basic, recurring employee cybersecurity training and a lack of testing system/data backups. These strengths and weaknesses were assessed using the **Identity Management**, **Authentication**, **and Access Control**, **Awareness and Training**, and **Data Security** categories under the Protect function of the NIST Cybersecurity Framework.

What are the recommendations for improving VB Tiki Tours' Protect Function?

Employees do not have work accounts, which can reduce the attack surface of an organization. However, this also means that there is no formal checking of an employee's cybersecurity knowledge. It is unknown whether or not employees can recognize phishing attacks, which is a major concern since VB Tiki Tours suffered a malicious phishing scam that resulted in the transmission of several unauthorized emails to the mailbox of VB Tiki Tours. It is highly recommended for employees to receive basic cybersecurity training; it does not need to be completely formalized. This can be as simple as a short discussion around phishing, business email compromise, and password security (CISA CPG Checklist, 2026). However, an alternative is to reinforce email security. These methods include using a Multi-Factor Authentication (MFA) system, enabling a built-in spam/phishing filter (e.g., Gmail), and since VB Tiki Tours has a custom domain/email, protocols like Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM), and Domain-based Message Authentication, Reporting, and Conformance (DMARC) can be set up. Cloudflare has a guide on SPF, DKIM, and DMARC, and CISA has a broader guide on email security. Additionally, DMARC Guide hosts a website to check whether or not a website has SPF, DKIM, and/or DMARC enabled. In terms of backup security, it is recommended to test the functionality of system or data backups on a periodic basis, whether that be weekly, bi-weekly, or monthly. It depends on the time constraints of the business. In the event that a cybersecurity incident occurred, and the backup is non-functional and contains data critical to continuing business operations, there will be heavy costs.

Detect (DE) Function

The fourth function is Detect (DE). The Detect function is focused on monitoring and the analysis of potential cybersecurity attacks and compromises (NIST, 2024). Solutions devised for

an organization's problems (defined in the PR function) are beneficial, but they are only beneficial if these problems occur in the first place. There is no sense in devising a counter to a rare, low-impacting threat; it is more important to monitor the threats that are likely to occur. Once the threat has been discovered, only then can the organization act and respond. A good execution of the Detect function means successful incident response and recovery activities (NIST, 2024).

We identified strengths and weaknesses in how VB Tiki Tours handles the Detect function. In terms of strength, VB Tiki Tours does monitor the physical environment to find potentially adverse events; mainly, the monitoring is dedicated to finding signs of trespassing and tampering with the previously owned Rum Shaker and the currently owned Rum Shaker II, which are both deemed as critical assets. Additionally, after VB Tiki Tours suffered from the phishing scam, they are actively seeking signs of attacks on email accounts. However, where there are strengths, there are weaknesses. One of these weaknesses is a lack of monitoring personnel activity and technology usage, though this is mainly attributed to the fact that there are no employee work accounts. Regardless, there is no formal checking of how employees conduct themselves while considering basic cybersecurity practices. These strengths and weaknesses were assessed using the **Continuous Monitoring** and **Adverse Event Analysis** categories under the Detect function of the NIST Cybersecurity Framework.

What are the recommendations for improving VB Tiki Tours' Detect Function?

After the Google review issue and the phishing scam, VB Tiki Tours is arguably anticipating another cybersecurity incident. However, whether or not employees (i.e., captains) are aware that they are a part of the attack surface is unknown. It is recommended, once again, to have a talk about basic cybersecurity practices (e.g., strong passwords, phishing training,

awareness). There is no need for an extensive cybersecurity training program, considering the time and budget constraints, but there should be a discussion on the potential for a cybersecurity incident to recur. If possible, since VB Tiki Tours uses Windows devices, Microsoft Defender Antivirus should be enabled by default. Additionally, a firewall should be activated by default too. If this is not the case, it is crucial that they are set up. The Detect function is mainly about awareness, so even periodically reviewing suspicious activities on email/bank accounts supports the Detect function.

Respond (RS) Function

The fifth function is Respond (RS). The Respond function is focused on the timeliness and ability of an organization to contain the effect(s) of a cybersecurity incident (NIST, 2024). This function includes outcomes such as "incident management, analysis, mitigation, reporting, and communication" (NIST, 2024). An improper execution of the Respond function can result in a broader or worse effect of a cybersecurity incident. When cybersecurity incidents occur, the organization should be communicative and organized enough to handle the incident with ease.

There was only one outcome discussed with VB Tiki Tours, and this outcome was related to one of their specific questions. We identified a particular weakness in VB Tiki Tours' Respond function. If an incident occurred, they did not know which entities to report to, and they did not have policies, procedures, or plans to respond to any particular incident. As a recommendation, we suggest contacting either the Cybersecurity & Infrastructure Security Agency (CISA) or the FBI's Internet Crime Complaint Center (IC3) in case a cybersecurity incident occurred. This outcome was assessed using the **Incident Response Reporting and Communication** category under the Respond function of the NIST Cybersecurity Framework.

Recover (RC) Function

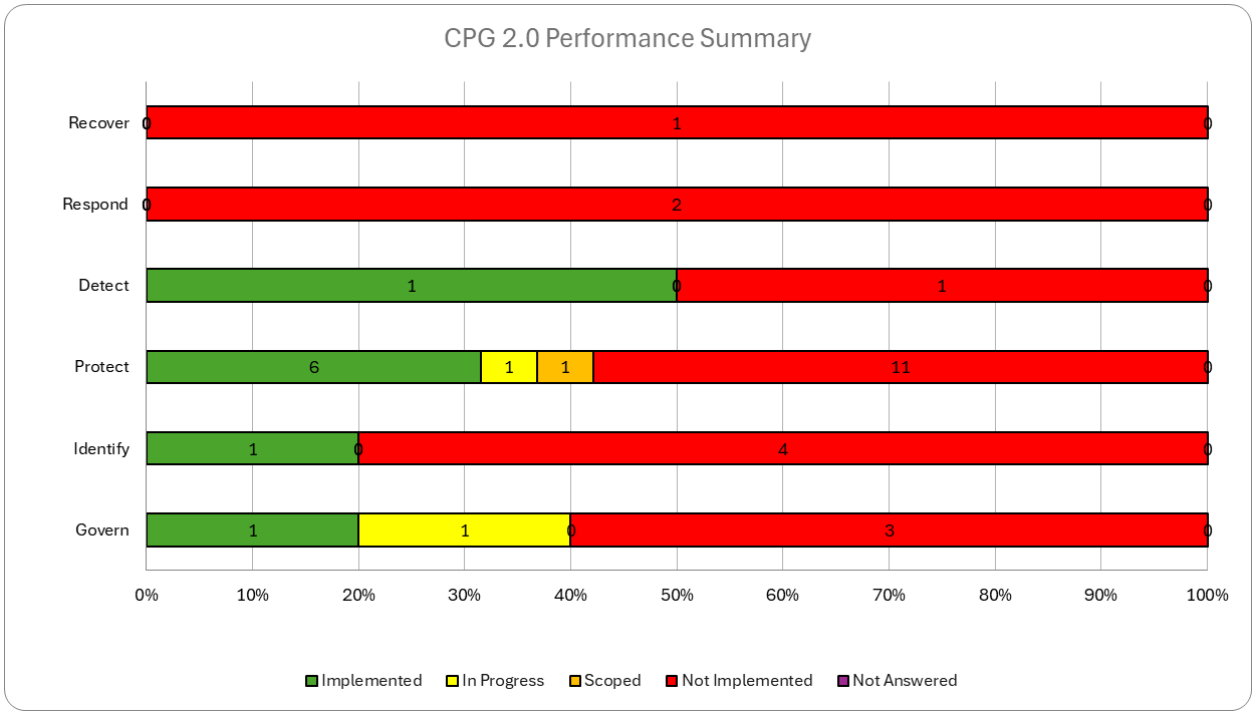
The sixth and final function is Recover (RC). The Recover function is focused on the restoration of the assets and operations affected by a cybersecurity incident (NIST, 2024). When cybersecurity incidents occur, it is likely that they will halt an organization's operations, sap recovery times, and destroy critical infrastructure or data that would otherwise keep the organization running. Knowing which authorities or agencies to report to, having multiple sources of backups, and constantly testing said backups can ease the recovery process in the event of a cybersecurity incident.

There was only one outcome discussed with VB Tiki Tours; we asked VB Tiki Tours whether or not an incident recovery plan had been drafted in the event that a cybersecurity incident occurred. In general, VB Tiki Tours is unable to execute any formalized/planned recovery operations, as there is no incident recovery plan drafted. Therefore, the recommendation, while considering the time and financial constraints, is to draft an incident recovery plan. IBM has a source on creating a disaster recovery plan (DRP), and Sprinto offers a guide in creating an incident recovery plan specifically for small businesses. Again, these are not mandatory, but investing some time in reading these guides, and VB Tiki Tours may recover tens of thousands of dollars in damage. This outcome was assessed using the **Incident Recovery Plan Execution** category under the Recover function of the NIST Cybersecurity Framework.

CISA CPGs

The CISA Cross-Sector Cybersecurity Performance Goals (CPGs) are practical, prioritized cybersecurity best practices for the protection of networks, systems, and data that guide actions and investments necessary to prevent and rapidly respond to cyber threats. For small and medium-sized businesses, NIST's Cybersecurity Framework can be daunting. The CISA CPGs simplify these recommendations by providing high-impact, low-cost measures that every organization can immediately begin adopting.

Using the CPG Workbook, we found that VB Tiki Tours has not implemented many practices under CPG 2.0. Considering the weaknesses that VB Tiki Tours currently faces, there are certain outcomes especially recommended to achieve as soon as possible. Additionally, these outcomes are achievable under VB Tiki Tours' time and financial constraints.



CPG 2.0 ID & Goal	Recommended Actions & Resources	Cost, Impact, & Ease
1.C Maintain Incident Response Plans	Considering that VB Tiki Tours does not currently have an incident response plan, if a cybersecurity incident were to occur, VB Tiki Tours may not be able to respond in a timely, orderly manner. This can result in financial loss too heavy for the business to bear. Once the incident response plan is established, policies for managing said plan are reviewed at least annually, updated when changes are applied, communicated, and enforced to reflect changes in requirements, risks, threats, technology, and organizational mission. The priorities within the IRP should be communicated to internal stakeholders (e.g., employees). Support Resources: https://www.cisa.gov/cisa-tabletop-exercise-packages https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r3.pdf	Cost = Low Impact = High Ease of Implementation = Moderate
3.F Implement Multifactor Authentication	Just like the incident response plan, VB Tiki Tours does not have any extra layer of security to protect the email account (info@vbtikitours.com) used for communication, which was subject to a phishing attack prior to VB Tiki Tours entering the Cyber Clinic program. Additionally, Mr. Hegrenes' (owner) personal laptop also functions as a work laptop, so some form of MFA would be beneficial in case the laptop is misplaced/lost and a threat manages to access the computer. Support Resources: https://www.cisa.gov/secure-our-world/turn-mfa	Cost = Moderate Impact = High Ease of Implementation = Moderate
	The work/personal laptop that Mr. Hegrenes uses is not currently equipped with a drive-wide encryption system, such as BitLocker Drive Encryption. This laptop, additionally, acts as a single-point-of-failure	

3.K Utilize Strong Encryption	since all files/data related to VB Tiki Tours is located on the aforementioned laptop. Depending on whether or not his Windows version is Pro or Enterprise, he may be able to activate BitLocker Drive Encryption. If not, it is highly recommended that he migrate his data to a secure cloud storage service provider. Support Resources: https://support.microsoft.com/en-us/windows/bitlocker-drive-encryption-76b92ac9-1040-48d6-9f5f-d14b3c5fa178	Cost = Moderate Impact = High Ease of Implementation = Complex
3.J Implement Cybersecurity Training	Although there are no work accounts for VB Tiki Tours' employees, they still represent a risk to VB Tiki Tours. They are part of the attack surface. There are no formal methods to assess their cybersecurity awareness (e.g., phishing recognition). The establishment of a multi-day, extensive cybersecurity awareness training program is not necessary, nor is it recommended. However there should be discussions on topics related to cybersecurity with VB Tiki Tours' employees (i.e., captains), even if the technicality of the incident is not the focus. Support Resources: https://www.cisa.gov/resources-tools/training https://www.cisa.gov/cybersecurity-training-exercises	Cost = Low Impact = High Ease of Implementation = Moderate
5.B Establish Incident Reporting Procedures	VB Tiki Tours had a large focus on non-cybersecurity related business operations over the past weeks. If an incident recovery plan is too time-consuming to create, VB Tiki Tours should know how and which entities to report to. Cybersecurity is not a solo effort. Having cybersecurity professionals examine a cybersecurity incident is better than a non-technical business leader handling an incident by themself.	Cost = Moderate Impact = High Ease of Implementation = Moderate

	Both CISA and the FBI's IC3 offer excellent service in assisting with cybersecurity incidents. Support Resources: https://www.cisa.gov/about/contact-us https://complaint.ic3.gov	

SWOT Analysis

What exactly is a SWOT analysis? SWOT is an acronym for Strengths, Weaknesses, Opportunities, and Threats. It is a simple strategic planning tool to understand an organization's current cybersecurity posture and what future opportunities to take and improve upon.

There are four key dimensions as mentioned before:

Strengths – What was done well.

Weaknesses – What needs to be worked on.

Opportunities – Chances for positive impact.

Threats – Risks that bring a negative impact.

VB Tiki Tours' SWOT Analysis

Strengths	**Weaknesses**
● Risk awareness concerning equipment ● Several physical measures used to protect assets (e.g., surveillance cameras) ● Up-to-date and obeys regulatory requirements (e.g., insurance) ● Usage of Standard Operating Procedures (SOPs) ● Usage of risk management plans	● Manual charging of surveillance cameras ● No cloud storage for camera footage ● No Multi-Factor Authentication (MFA) ● No firewalls on critical assets ● Limited backups ● No testing of backups ● Single-point-of-failure in a device (i.e., all business files are stored on laptop) ● Limited budget on IT staff ● Lack of cybersecurity policies
Opportunities	**Threats**
● Autonomous charging of cameras (e.g., solar power) ● Business-grade cloud storage and backup (e.g., Backblaze) ● Creating cybersecurity incident response/recovery plans ● Documenting risk tolerance ● Inventory third-party services ● Research cyber threat intelligence (i.e., good source of cybersecurity news/updates)	● Attacks on Wix website (e.g., SQL Injection) ● Phishing scams and social engineering attacks ● Physical tampering with assets (i.e., the Rum Shaker II) ● Third-party supplier risk (e.g., Fareharbor) ● Compliance issues (e.g., boating license) ● Data breaches

Next Steps

VB Tiki Tours Questions and Recommendations

This section specifically covers your initial questions and our team recommendations.

What Is Cybersecurity, and What Are Some Basic Information Regarding Cybersecurity?

Cybersecurity is the practice of protecting your computers, systems, and sensitive information like customer data, passwords, and financial records from digital threats. Cyberattacks often start with small, simple tactics such as phishing emails or exploiting outdated software, so basic precautions go a long way. Using precautions such as keeping your systems updated and requiring strong passwords with multi-factor authentication can significantly reduce risk. It's also important to train employees to recognize suspicious links or attachments, since human error is one of the most common entry points for attackers. Even small businesses are targets, so having these basic protections in place helps prevent data loss, financial damage, and downtime.

How to Avoid or Be Aware of Phishing Attacks?

There are many ways to avoid phishing attacks. This includes the following: verifying the grammatical/typographical correctness of the email's content within the header and body of the message. False/phishing emails typically have incorrect grammar, unprofessional formatting, odd misspellings, and suspicious email attachments. The Federal Trade Commission has a guide on how to recognize phishing scams and how to respond if you become a victim of one.

Who to Report to in the Event of a Cyber Attack?

Cyber professionals should be relied upon rather than trying to take it on yourself. We specifically recommend the Cybersecurity & Infrastructure Security Agency (CISA) since CISA is a group of cyber professionals and is available 24/7. On top of that, CISA will also remain confidential about the information that you relay to them. Additionally, the FBI has its own incident-reporting website called the Internet Crime Complaint Center (IC3) in the event a cyber-enabled crime occurred (e.g., cyber fraud).

How Do I Implement Cyber Risk Management Practice?

We first recommend identifying critical/non-critical assets within VB Tiki Tours and identifying potential risks to the aforementioned assets, then assessing these risks by evaluating their likelihood (how likely the risk will manifest) and impact (how damaging the risk will be if it manifests). COMPLYAN has a short article on cyber risk management practices. However, in short, if the risk's likelihood is high, and the impact is also high, then the countermeasures for this risk should be prioritized.

There are four strategies to deal with these risks:

- Avoid: Eliminate the risk entirely by discontinuing risky activities or removing vulnerable assets.
- Transfer: Shift the risk to another party through insurance or outsourcing.
- Accept: Acknowledge certain risks as acceptable given their low likelihood or impact.
- Mitigate: Implement controls to reduce the probability or impact of threats.

Overall, the best way to implement cyber risk management practices is to review the outcomes within the NIST CSF 2.0 and the CISA CPGs since they offer a view of what "perfect" security appears like. How these outcomes are achieved is based upon your discretion; for the sake of self-sustainability, and since an in-house or third-party cybersecurity team is costly, we recommend using artificial intelligence (e.g., OpenAI's ChatGPT) to generate methods on how to achieve these outcomes.

What Are Malware Infections?

Malicious software, better known as malware, is a computer program designed with the intention of damaging another system. Below are the types of malware infections we went over and how we described them:

- Virus – Attaches to files and spreads when files are opened
- Worms – Spreads across networks autonomously
- Trojan – Disguises itself as legitimate software
- Ransomware – Locks files and demands payment
- Spyware – Secretly tracks user activity or steals data
- Adware – Flood a device with unwanted advertisements

There are several ways to deal with malware, but the most common method is the usage of an antivirus program. If your personal/work laptop runs Windows, it is likely that it is running Microsoft Defender by default, which is free and efficient. Otherwise, refrain from accessing/clicking e-mails and texts from unknown contacts.

How to Respond to Cyberattacks and Create a Cybersecurity Incident Response Plan?

Cybersecurity incident response plans are the solution to properly responding to cyberattacks. Since the team lacks the in-depth, insider knowledge of the organization to create a comprehensive cybersecurity incident response plan as a deliverable, it is best for you to draft it themselves. It is not mandatory for the response plan to be extensive. Conciseness is better. The SANS Institute and the Department of Health and Human Services provide templates on cybersecurity incident response plans.

These plans are specific to a single organization. In essence, these are playbooks for when certain cybersecurity incidents occur within a certain organization. From the SANS Institute (n.d.), there are seven stages in an Incident Response Life Cycle Process (i.e., the incident response plan):

1. **Preparation** - Ongoing process of maintaining/improving incident response capabilities by securing a business's systems and training employees on cybersecurity awareness.
2. **Identification** - Determine and confirm what particular incident occurred and what assets have been affected (e.g., the Rum Shaker II's cameras).
3. **Notification** - Alert employees involved in the incident response plan to the occurrence of a particular incident while maintaining active communication.
4. **Containment** - Minimize financial or reputational loss, theft of information, and disruptions to service (e.g., the Wix website VB Tiki Tours is hosted on).
5. **Eradication** - Eliminate the threat, such as by using an antivirus (e.g., Microsoft Defender Antivirus).

6. **Recovery** - Use backups to restore business operations and services to return to a normal state of operation.
7. **Post-Incident Activities and Reporting** - Assess the overall performance of the response to the cybersecurity incident (i.e., cyberattack) and note 'lessons learned.'

In the event that an incident occurs and a cybersecurity incident response plan has not yet been drafted, the best solution would be to immediately contact law enforcement (e.g., the FBI's IC3, Virginia State Police, and CISA) in the event of a cyberattack.

Data Breaches and Storage Reconnaissance?

Hackers perform reconnaissance before attacking, as they often look for the weakest link to exploit. Analogy-wise, they pick the lowest-hanging fruit. Hackers usually search for weak emails, passwords, credentials, or a lack of general security and network security. Without any network monitoring tool, such as Wireshark, and a professional network analyst, it will be hard to detect intrusions into VB Tiki Tour's network and the personal/work laptop.

On a more advanced, technical, and costly level, one solution that can be used against any attackers performing reconnaissance on your networks is to use either an Intrusion Detection System (IDS) or an Intrusion Prevention System (IPS). Either or, these solutions "simply monitor and report suspicious activity and traffic when they detect an anomaly" (Fortinet, 2025).

If you suspect that your email has been in a data breach, the Have I Been Pwned website can verify it.

Overall Conclusion

The work of your business is impressive. Our team learned many strengths and areas of improvement within your company, and we are interested in your continued success. After reviewing the NIST, CPG 2.0, Valor Top 10 and SWOT analysis, we believe VB Tiki Tours will be more secure. These risk assessments highlight that while VB Tiki Tours has taken meaningful initial steps toward securing its physical assets and maintaining business operations, several critical gaps in its cybersecurity posture must be addressed to ensure long-term resilience. As a growing small business operating within the hospitality industry, VB Tiki Tours faces increasingly common and inevitable cyber threats such as phishing, ransomware, and denial-of-service attacks.

Through the application of frameworks such as NIST Cybersecurity Framework 2.0 and CISA Cybersecurity Performance Goals, our team identified both strengths, such as asset inventory and physical security measures, and weaknesses, including limited employee training, inconsistent backup practices, and a lack of formalized cybersecurity policies. These gaps, while common among small businesses, present risks to business operations, customer trust, and financial stability if left alone.

Our recommendations are practical, low-cost, and scalable solutions tailored to the VB Tiki Tours' size and resources. By improving employee awareness, implementing stronger email and authentication protections (i.e., MFA), formalizing risk management practices, and adopting reliable backup and monitoring systems, VB Tiki Tours can significantly enhance its security posture.

Ultimately, cybersecurity is not a one-time effort but an ongoing process that requires constant re-evaluation. By taking steps now, VB Tiki Tours can reduce its exposure to cyber threats and provide enjoyable experiences for its customers without worrying about costs.

List of Future Best Practices/Recommendations

This section is a condensed version of the recommendations provided throughout the report, including sections such as the Valors Top 10 Checklist, the NIST CSF 2.0, and the CISA CPG 2.0.

- Use a **cloud service**, such as Google Drive, for storage and backups.
    - Test the functionality of backups periodically, whether that be weekly, bi-weekly, monthly, or bi-monthly.
    - Follow the 3-2-1 rule for backups.

- Implement basic cybersecurity awareness training for employees.
    - Alternatively, simply discuss what employees know regarding cybersecurity. What have they heard on the news? Do they consider cybersecurity while working?
    - Focus on recognizing phishing, practicing strong password hygiene, and understanding basic cyber threats such as malware.

- Implement an added layer of security when logging onto accounts, such as a **Multi-Factor Authentication (MFA) system**.

    - On cellular devices, consider opting for passwordless authentication (e.g., biometric).

- Establish and maintain a simple cybersecurity incident response plan for highly anticipated incidents (e.g., phishing scam).

- Secure **email systems.**
    - Enable spam and phishing filters.
    - Configure domain protection protocols such as SPF, DKIM, and DMARC.

- Formalize **risk management practices.**
    - Define risk tolerance levels.
    - Define basic cybersecurity policies.

- Inventory **assets** and **third-party services**.
    - Track digital and physical assets.
    - Track third-party services (e.g., Fareharbor).
    - Prioritize protection of assets based on criticality.

- Use **antivirus software** and network firewalls on all devices
    - Review suspicious account activity (e.g., logins from other nations).

    - Depending on what Internet Service Provider (ISP) you use, such as Verizon or Cox, they have different ways of setting up the firewall on the router/modem.

- Depending on what data you handle and you become a victim of a cybersecurity incident (i.e., cyber attack), stay familiar with **federal** and **Virginia's data privacy laws**.
    - Virginia has the Virginia Consumer Data Protection Act (VDCPA) and the Virginia Personal Data Breach Notification Law (VPDBNL).
    - Health Insurance Portability and Accountability Act (HIPAA).
    - Federal Trade Commission Act (FTCA)

- Stay **up to date** on **cybersecurity news**, such as:
    - The Hacker News.
    - Reuters Cybersecurity.
    - Cyber Security News.

- Report to the following **law enforcement agencies** if a cybersecurity incident occurred:
    - FBI's IC3.
    - Virginia State Police.
    - CISA.

References:

Agarwal, S. (2026, February 26). *What Is the Hospitality Industry? Definition, Sectors & Importance (2026 Guide)*. Sara Hospitality USA. https://sarahospitalityusa.com/blog/what-is-the-hospitality-industry

BOD 18-01: Enhance Email and Web Security | CISA. (2017, October 16). Www.cisa.gov. https://www.cisa.gov/news-events/directives/bod-18-01-enhance-email-and-web-security

CISA CPG Checklist. (2026, March 20). Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/sites/default/files/2023-03/cisa_cpg_checklist_v1.0.1_final.pdf

Cloudflare. (2023). *What are DMARC, DKIM, and SPF?* Cloudflare. https://www.cloudflare.com/learning/email-security/dmarc-dkim-spf/

Code of Virginia Code - Chapter 53. Consumer Data Protection Act. (2023). Virginia.gov. https://law.lis.virginia.gov/vacode/title59.1/chapter53/

Cybersecurity and Infrastructure Security Agency. (n.d.). *About CISA*. Cybersecurity and Infrastructure Security Agency CISA. https://www.cisa.gov/about

Fortinet. (2025). *What is an Intrusion Detection System (IDS)?* Fortinet. https://www.fortinet.com/resources/cyberglossary/intrusion-detection-system

HHS. (2023). *Cybersecurity Incident Response Plans*. https://www.hhs.gov/sites/default/files/cybersecurity-incident-response-plans.pdf

IBM. (2023, November 30). *Disaster Recovery Plan*. Ibm.com. https://www.ibm.com/think/topics/disaster-recovery-plan

Internet Crime Complaint Center (IC3). (2023, November 8). *Ransomware - Internet Crime Complaint Center (IC3)*. Ic3.Gov. https://www.ic3.gov/CrimeInfo/Ransomware

Internet Crime Complaint Center (IC3) | Home Page. (n.d.). Www.ic3.Gov. https://www.ic3.gov

Itkin, L., Ravich, L., Zaidenberg, O., Winther, P., & Cook, S. (2025, October 24). *Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®*. Attack.mitre.org. https://attack.mitre.org/techniques/T1566/

Marino, M. (2025). Cybersecurity Threats and Their Impact on the Hospitality Industry. *International Journal of Gaming Hospitality and Tourism*, *5*(1). https://stockton.edu/light/documents/ijght_vol.5no.1/cybersecurity_threats_and_their_impact_hospitality_industry_9.8.25.pdf

National Institute of Standards and Technology. (2022, January 11). *About NIST*. NIST. https://www.nist.gov/about-nist

NIST. (2024). The NIST cybersecurity framework (CSF) 2.0. *The NIST Cybersecurity Framework (CSF) 2.0*, *2.0*(29). https://doi.org/10.6028/nist.cswp.29

Oliveira, A., Fiser, D., Logan, M., Manral, V., & Weizman, Y. (2025, October 24). *Endpoint Denial of Service, Technique T1499 - Enterprise | MITRE ATT&CK®* Attack.mitre.org. https://attack.mitre.org/techniques/T1499/

SANS Institute. (n.d.). *Cyber Security Incident Response Plan Cyber and Data Security Incident Response Plan Template*. https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-Response-Template.pdf

Statista Research Department. (2026). *Topic: Travel and Tourism Industry in the U.S.* Www.statista.com; Statista. https://www.statista.com/topics/1987/travel-and-tourism-industry-in-the-us/