Team 5 Final Project: MGM Resorts

Risk Management Assessment

CYBR 658 : Risk Analysis and Compliance

University of Maryland Baltimore County

Presented to: Professor Ronald Nemes

Presented by: Aaron Roberts, Alan Weiss, David Kim, Erin Fago, and Greg Brown

Thursday, December 16th, 2021

Table of Contents

Executive Summary

Team 5 has created a Risk Management Plan for the Hotel Reservation System at MGM Resorts International. In our Business Impact Analysis, we identified that MGM's core business function is to provide constant availability of the IT systems that allow customers to purchase hotel reservations online. We identified that this should have a maximum tolerable downtime of 2 hours and a recovery time objective of 1 hour. Numerous threats such as data exfiltration and ransomware impact downtime. In order to mitigate these risks, we recommend a holistic approach that leverages employee training as well as clear, written policies and procedures that are championed by senior management. In addition, we recommend upgrading IT infrastructure to include up-to-date physical security tools such as server room locks and software tools including next-generation firewalls and antivirus software. Administrative processes such as terminating accounts for any persons who no longer require access will also help protect the integrity of our systems. Crucially, we stress that it is no longer sufficient to leave cybersecurity to one group. Effective protection of IT systems from malicious actors requires organizational cybersecurity awareness and steadfast support from both C-suite executives and technical employees at all levels of experience.

Risk Management Plan Outline and Research

Introduction

MGM Hotels and Casinos operates 29 hotels in the United States and Macau serving customers from around the world. Our existing risk management plan for the hotel reservation system is outdated and puts the company at significant risk. Access to systems and data is not properly secured which leaves us open to data being compromised or stolen. Inadequate security controls and training leaves us vulnerable to malware and ransomware. In addition, our lack of adherence to key regulations puts us at risk for significant fines from governments in both the United States and Europe.

In order to mitigate the risks above, we propose creation and implementation of a new risk management plan that will greatly increase our data security and reduce our exposure to bad actors and government regulations. In order to prepare for this, we researched best in class risk management approaches and settled on the plan described below.

Approach

There are a number of risk management approaches that are widely in use. One of the most popular and comprehensive approaches has been defined by the National Institute of Standards and Technology (NIST). Although it was originally intended for government use, it can be applied to large organizations as well. The framework consists of seven activities that we will perform. They are:

1. Prepare - Essential activities to prepare the organization to manage security and privacy risks

2. Categorize - Categorize the system and information processed, stored, and transmitted based on an impact analysis
3. Select - Select the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
4. Implement - Implement the controls and document how controls are deployed
5. Assess - Assess to determine if the controls are in place, operating as intended, and producing the desired results
6. Authorize - Senior official makes a risk-based decision to authorize the system (to operate)
7. Monitor - Continuously monitor control implementation and risks to the system

Scope and boundaries

Per instructions from management, the risk management plan will be limited to the hotel reservation system. It will not focus on gambling operations, restaurants, or other services provided by MGM. It will include both B2B activities such as reservations through 3rd parties such as Expedia and Hotels.com as well as reservations booked directly through their phone or online reservation systems.

The plan will address the data centers that house the web, application, and database servers that support the reservation system as well as the workstations on hotel premises that are used by hotel staff to add, update, or delete reservations. The data centers include the primary data center as well as the data center that houses our hot backup. In addition, it will address the internal network, external network and the DMZ. The plan will not address devices that are used to remotely access the reservation

system or the data center. Those devices are covered under plans for all remote devices, regardless of what functions they support. It will also not address servers on hotel properties such as mail and file servers as those are used for many purposes beyond hotel reservations.

Compliance/Laws

There are three sets of regulations that we must adhere to in order to keep customer data safe and stay in compliance with European and American regulators. Failure to comply with any of these could result in misuse of customer data, significant penalties, and reputational damage. These three sets of regulations are the General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Payment Card Industry Data Security Standard (PCI DSS).

Key provisions of each of the three sets of regulations are described below:

1. GDPR (Bhatia, 2021)
    a. Collect only data that is necessary for the transaction
    b. Allow customers to request that personal data be deleted once transaction is complete
    c. Maintain personal data breach register
    d. Report breaches within 72 hours
    e. Must have a Data Protection Officer
    f. Create awareness and training for employees
2. CCPA (Gilbert, 2021)
    a. Provide notice to consumers before collecting personal data

b. Allow consumers to opt out, read, delete their personal data from business's storage
c. Verify the identity of consumers who ask to read and delete their information

3. PCI DSS (Exabeam, 2021)
    a. Maintain a firewall
    b. Passwords must be unique
    c. Protect stored data
    d. Use and update antivirus software
    e. Develop and maintain secure systems and applications
    f. Restrict access to cardholder data
    g. Restrict access to systems holding sensitive data
    h. Restrict physical access to cardholder data
    i. Track and monitor access to network resources and cardholder data
    j. Regularly test security systems and processes
    k. Maintain a security policy

Roles and Responsibilities

For a large organization such as MGM, it is critical to have responsibility for risk management spread among multiple people and teams. A detailed breakdown of the roles and responsibilities that will be necessary to carry out the recommended actions can be found in the Risk Assessment section.

Proposed Schedule

Due to the significant risk the organization currently faces, it is critical that we define and get approval for our risk management plan as quickly as possible. Therefore, we have established the following schedule for documenting and socializing our plan:

a. Introduction - 10/21
b. Risk Assessment Plan - 10/28
c. Risk Mitigation Plan - 11/11
d. Business Impact Analysis - 12/2
e. Business Continuity Plan - 12/2
f. Submission of Final Plan - 12/16

Risk Assessment

Outline

a. Introduction
b. Define the Scope & Boundaries
c. Identify assets and activities of the Data Center
d. Identify relevant Threats & Vulnerabilities
e. Identify relevant controls
f. Identify Key roles and Responsibilities of Departments and employees within the Company
g. Final Risk Assessment

Introduction

With the overview and schedule of our risk management plan provided, we will begin with the risk assessment. Within this document the various assets relating to the hotel booking system of MGM Casino will be identified. These assets will then be evaluated to isolate the threats and vulnerabilities which are related to each. The impact of a threat or vulnerability in regards to downtime, cost, customer trust, etc. will then be displayed. Once completed, the controls that should be implemented to reduce or avoid these risks will be discussed. These controls tie directly to the key roles and responsibilities of the departments and employees within MGM Casino in order to ensure secure operations. The creation of this risk assessment provides MGM Casino with knowledge of their attack surface in order to develop countermeasures to continue business safely and effectively while reducing vulnerabilities and supporting decision making by prioritizing risk.

Scope & Boundaries

The risk assessment plan will focus on the threats and vulnerabilities associated with MGM Casinos hotel reservation system within their internal network (database servers, corporate network) as well as their DMZ (i.e web server, guest network). In addition, the assessment will evaluate the external network in regards to third party reservation sites (Airbnb.com, Expedia.com, Booking.com, Hotel.com, etc.).

Data Center Assets & Activities

Assets	Activities
- Servers (Databases, Email, Corporate, Guest, etc.) - Employees - Hard Drives - Routers - Switches - Operating Systems - Website domain / application	- Data Storage / Backups / Recovery / Management - eCommerce - Enterprise Resource Planning (ERP) / Customer Relationship Management (CRM) - Web Domain Management - Database server frequently accessed from the web server

Threats & Vulnerabilities

Threats	Vulnerabilities	Harmful Event or Loss
- Lost / Stolen Company Data & Assets	- Improper hardware sign out policy - Improper data center access tracking - Improper company asset guidelines - Hardware being removed from production systems	- Loss of financial data - Loss of data confidentiality - Loss of consumer trust

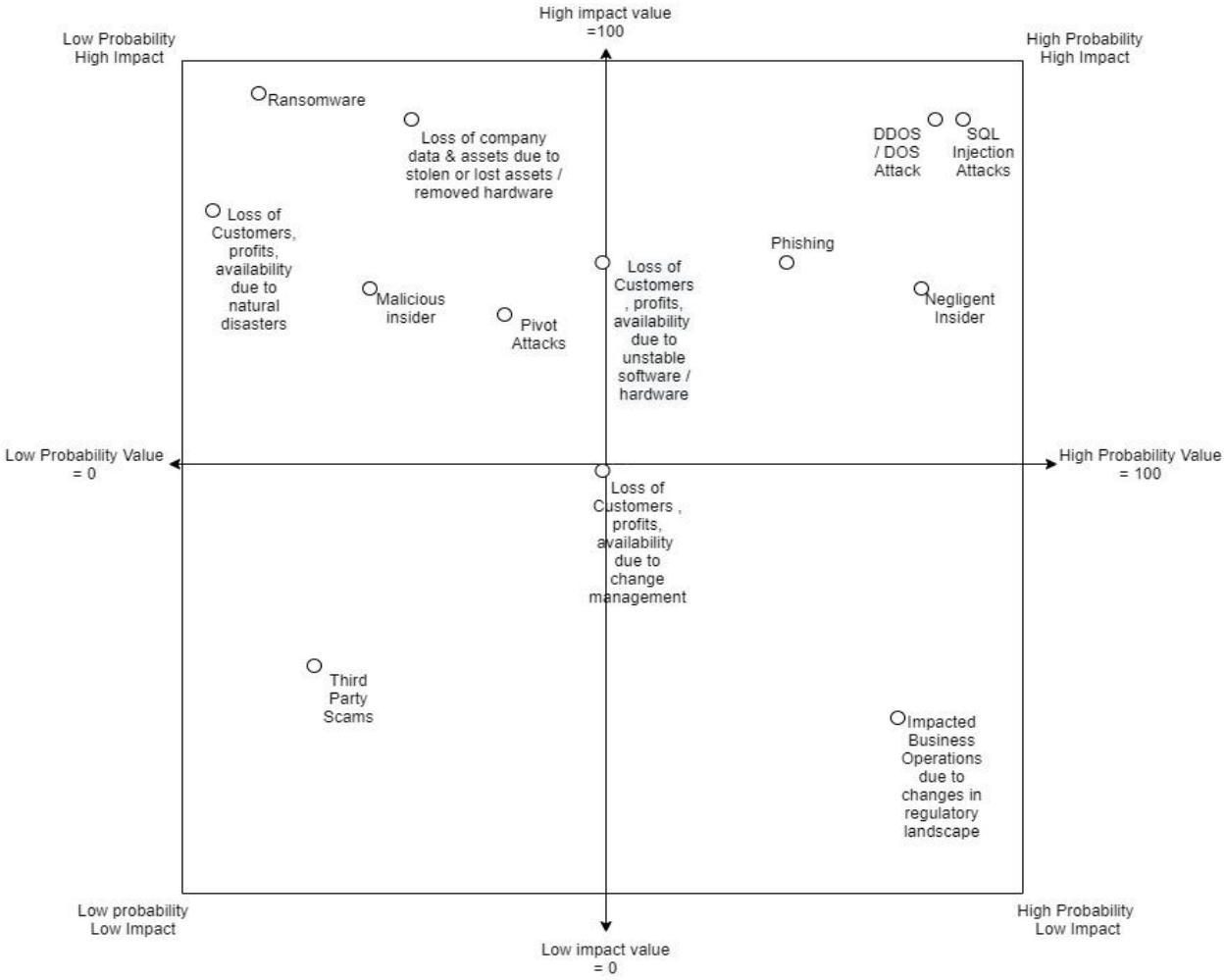
- Natural Disasters
  - Hurricane
  - Tornado
  - Heat Waves
	- No warm or hot site in case of damage to the main data center
	- Lack of backup power supplies
	- Lack of data backups
		- Production Outage:
		  - Loss of customers
		  - Loss of profits
		- Decrease in availability / reliability
		- Data Loss
		- Physical Loss

- Change Management
  - New Policies
  - New Systems
  - New Structure
- Regulatory Landscape Altered
	- Untrained employees
	- Lack of planning
	- Lack of redundancy
		- Decrease in availability / reliability
		- Mistakes due to learning curve
		- Servers / Sites temporarily offline
		- Potential fines

- Unstable Software / Hardware	- Inadequate input validation / sanitization
	- Operating software with known vulnerabilities
	- Unpatched and out-of-date applications
		- Production Outage:
		  - Loss of customers
		  - Loss of profits
		- Decrease in availability / reliability
		- Data Loss
		- Physical Loss

- Spam - Malware - Phishing - SQL Injection attacks , Buffer Overflow attacks, DDOS / DOS attacks - Ransomware - Data breaches / Leaks - Pivot attacks by utilization of the guest network	- Inadequate input validation / sanitization - Lack of / Improper employee cyber awareness training - Network hardware / software not properly documented - Company products being accessible on the Internet	- Data Loss - Loss of data confidentiality - Loss of customer trust - Loss of availability / reliability - Stolen PII - Loss of Trust
- Malicious Insider	- Improper handling of separation of duties - Lack of / Improper termination policy - Unlocked computers - Unlocked server rooms - Improper implementation of principle of least privilege	- Data Loss - Loss of data confidentiality - Loss of availability / reliability - Asset loss - Stolen PII
- Negligent Insider	- Lack of / Improper employee cyber training - Overworked Employee - Inadequate training - Honest Mistakes	- Data Loss - Loss of data confidentiality - Loss of availability / reliability - Asset loss

- Compromised Third Party Booking Sites	- Insecure third party providers - Lack of research / follow-up in regards to utilized third party systems	- Loss of PII - Loss of Customers - Loss of Trust - Loss of income



Control Types

Controls	Preventative	Detective	Corrective
Physical	- Server room locks - Smart Card Reader	- CCTV - Cameras	- Repair preventative and detective equipment in a timely manner - Install necessary equipment in unsecure rooms ASAP
Technical	- Firewalls	- IDS	- Implement Software patches &

	- Spam filters - Antivirus - Tools - IPS - Redundancy	- Vulnerability Testing - Penetration Testing - Honey Pots	Updates ASAP - Perform proper Input validation - Continuously keep firewall rules up to date
Administrative	- Separation of duties - Data Classification - Termination Policies - Principle of Least Privilege	- Evaluate personnel access - Evaluate logs	- Remove employee access as necessary - Implement principle of least privilege - Incident Response plan

Roles & Responsibilities

Roles	**Responsibilities**
Upper Management	- Evaluate the risk assessment to make financial determinations of where money should be allocated to various business areas for secure operations.
CIO (Chief Information Officer) (Stevens, 2016)	- Awareness of regulations in regards to the business operations of MGM Casinos - May be responsible for leading cyber awareness training sessions - Create a cyber security benchmark based off of guidelines such as NIST - Manage cyber security controls of that of third party vendors
Managers	- Promote the importance of following security protocols to their employees and peers - Document Cyber Security related incidents and report to the appropriate department or individual
ISSO (Information Systems Security Officer) (Chron, 2020)	- Writing security policies - Leading cyber awareness training sessions - Manage access controls - On-boarding & off-boarding employees - Recovery Plan
IT Specialists: - Vulnerability / Penetration Testers - Information Assurance	- Perform proper input validation and error handling - Evaluate system and access logs regularly - Update access controls - Secure network configuration

Engineers - Software Developers - Network Engineers - Database Administrators	- Back ups - Identify vulnerabilities, threats and faults - Follow / Perform the documented incident response plan
Data Entry Personnel	- Ensure accurate data is being entered - Follow cyber security guidelines as instructed by Quality Assurance professionals - Follow acceptable use policy when utilizing the company's Information systems
Quality Assurance	- Assign Cyber Awareness training to employees on a scheduled basis and document who has or hasn't completed the training - Distribute the acceptable use policy to employees and request a signed copy back - Perform proper on-boarding and off-boarding procedures
Third Party System Owners - Software Companies - Hardware Companies - Hotel Booking Sites	- Secure their systems - Provide a secure and safe system for various companies to utilize - Provide patches, updates and repairs as soon as vulnerabilities are found and corrected. - Provide reliable availability to their users

Schedule

Date	**Task**
October 09, 2021	Research
October 09, 2021	Outline
October 10, 2021	Introduction
October 11, 2021	Scope & Boundaries
October 12, 2021	Identify Assets
October 15, 2021	Identify Threats / Vulnerabilities
October 20, 2021	Identify Controls
October 22, 2021	Identify Roles / Responsibilities

Risk Mitigation

Outline

1. **Introduction**
2. **Threats**
    a. Data exfiltration of customer's personal information or data leakage of confidential business records - (red)
        i. Phishing campaigns
    b. Insider threat (malicious and negligent) - (red)
    c. Distributed Denial of Service (DDoS) - (yellow)
    d. Malware (including viruses, keyloggers and ransomware) - (yellow)
    e. Natural disasters (fire, flood, power outage) - (green)
3. **Migitations**
    a. Employee training and/or hiring costs
        i. Real-time data monitoring and comparison to established baseline
    b. Clear, simple and irrefutable written user policies
    c. Content delivery networks, scheduled backups, load balancing
    d. Properly installed and configured technical environment (firewall, IDS, IPS, workstations) with up-to-date software patches and firmware
    e. Hot/cold site and failover power design
4. **Discussion and General Recommendations**
    a. Intangible Costs
        i. Reputational damage

Introduction

The purpose of this risk mitigation report is to identify what threats are most likely to disrupt the normal function of the online e-commerce hotel reservation system at MGM Resorts International, and clarify what steps business leaders can take in order to mitigate the risks of operating in such a hostile environment. With the goal of providing guidance that is practical and clear, the relative priority of each threat category has been designated a ranking according to the following general risk formula.

Risk = Threat x Vulnerability x Asset (Gibson)

It is important to recognize this formula does not operate with absolute numerical inputs, but rather serves to model risk in a qualitative manner based upon 3 factors - the existence of vulnerabilities (as defined in the Risk Assessment) within MGM's operating IT environment, the willingness of a human threat actor or organized criminal group to exploit those vulnerabilities, and finally, the dollar-value of business assets (like servers) that support the normal function of the hotel reservation application on MGM's website.

Ranking Methodology

The most severe threats are coded as red. These threats are most likely to occur and also cause substantial revenue loss (frequency-high, impact-high). Significant threats that occur slightly less often and cause moderate revenue disruption are coded in yellow (frequency-moderate, impact-high to moderate). Finally, threats categorized as green occur least frequently, or occur in a manner that is predictable, and so these risks can more readily be mitigated in-advance (frequency-low, impact- moderate to low).

Threats

a-b.) Red-level threats - The risk management team considers data exfiltration of customers' personal information and leakage of confidential business records to be the most significant threats facing the online hotel reservation system at MGM Resorts International. Phishing campaigns and insider threats often lead to exfiltration of this same data, and so these threats have also been included in the most severe category (Verizon DBIR, 2020).

In today's operating environment, customers are significantly more aware that businesses collect and store the personal information of their end-users. Possible

examples of such data in MGM's hotel reservation systems include the date of birth of individual customers, residential addresses, payment information, hotel visit frequency, spending habits, internal rewards tier, and relationships to VIP persons (MGM Reports) The backlash that MGM and its business partners would face upon leakage and publication of this personally identifiable information (PII) would be severe. There exists a long history of regulators issuing punishments for instances of data compromise in the e-commerce industry. In March 2018, Expedia was fined $110,000 and issued a civil penalty for exposing the personal data of 20,755 customers in Pennsylvania (Coble, 2019). More recently, Equifax settled with Illinois for $19.5 million USD after being accused of inadequately storing data representing driver's license and social security numbers (Cobble, 2020). These cases indicate a trend toward greater scrutiny of internal IT practices by external regulators, along with the likelihood of higher fines in the future.

c-d.) Yellow-level threats - Denial-of-Service (DoS) attacks and ransomware attacks are two very significant threats that fall into the moderate risk prioritization category. In a DoS attack, the online hotel reservation application hosted on MGM's computer servers is rendered inaccessible to normal customers due to a flood of requests by an attacker. When an attacker leverages millions of devices located across the world prior to initiating requests to MGM's hotel reservation website, the DoS attack is considered distributed (DDoS).

Ransomware is a very different kind of attack that also renders MGM's hotel website inaccessible to regular customers. In a ransomware attack, the files required for regular business use hosted on MGM's web application servers become encrypted due to malware that has found its way onto MGM's internal network devices. Encrypted files cannot be read, written to, or executed. According to a report conducted by Cisco, the average amount paid by ransomware victims in 2020 was $312,493 - representing a 171% increase year-over-year (Ackerly, 2021).

e.) Green-level threats - Hurricanes, tornadoes, floods, fires and earthquakes are all possible natural disasters that have the capacity to disrupt the functioning of MGM's hotel reservation website (Idx.us). If the data center hosting MGM's content is taken offline due to a power outage, then regular business operations involving the website would also be disrupted. Therefore, adequate risk mitigations must be prepared beforehand.

Mitigations

a-b.) Data exfiltration of confidential business records and customers' personal information poses a severe risk to MGM Resorts' hotel e-commerce platform. Luckily, many concrete interventions exist that help mitigate this risk to an acceptable level. While it is true employees are crucial to the success of any business, they are also one of the biggest sources of cybersecurity vulnerabilities.

The single most effective risk mitigation strategy involves employee training and working with the internal IT team to establish a culture and mindset that reinforces the relevance

of cybersecurity to everyday job tasks. This cybersecurity training control boosts network security defenses and achieves this result at lower time-cost expense than hiring a new team of subject matter experts. Once an internal IT team has been trained, they can establish a baseline for what their regular hotel reservation network traffic looks like. Then unusual or malicious data exfiltration traffic can be detected and correspondingly eradicated. Simulation is also an effective educational tool. Many specialized vendors offer “security awareness training platforms” that can simulate phishing emails in a protected environment that helps employees better identify the telltale characteristics of a scam.

Finally, the direct involvement by senior management to establish clear, written policies and procedures should not be underestimated as an effective risk mitigation technique. It is crucial that senior management and technical IT staff are on the same page regarding everyday business practices. These include standard protocols for centralized logging, data backups, patch management, and deactivation of terminated employees accounts. These actions can help reduce the impact of insider threats since ex-employees are no longer able to access proprietary company data.

c-d.) The mitigations that exist for DDoS and ransomware attacks are grounded in establishing reliability and availability of hotel reservation services to end users. Load balancing is one possible solution that improves network response times to requesting clients. Cloudflare offers these replication and redundancy services to hosted web server applications on the enterprise-scale required by MGM. In the event of a DDoS

attack, the redundancy of Cloudflare's web servers still provides uninterrupted service to MGM's customers because even if one (or more) CDN servers go offline, network traffic can be evenly redistributed across those servers that remain operational (Cloudflare).

Next, ransomware is most effectively mitigated by maintaining a regular data backup schedule and practicing the procedures to restore from those backups. The effectiveness of ransomware becomes severely diminished if the victim has another copy of the encrypted data, and they can simply restore from a snapshot instead of paying for an unreliable decryption key. Many different techniques to backup data exist (on-premises vs. in-the-cloud, RAID configuration, and full vs. incremental vs. differential backup); however, the exact method matters less than its reliability. Stored data backups also must be tested to determine if data restoration would be successful under a disaster scenario. Companies should strive for a success rate greater than 95% in order to have realistic confidence their data can be restored (Gibson, Darril).

e.) Electricity failover power designs should be implemented when attempting risk mitigation against natural disasters. This way, even if a fire, flood, or power outage affects one of the server clusters, other failover servers that were placed on a different power grid (and perhaps also located in a different physical location) remain functional and online. While no power arrangement guarantees 100% uptime, design choices that incorporate server and power failover are less likely to have both plans fail.

Discussion and General Recommendations

Preparation for cybersecurity threats in-advance helps to mitigate risks that otherwise would disrupt the normal functioning of MGM's hotel e-commerce website. It is important to implement risk management against threats that have a high probability of occurring. The losses associated with data exfiltration or ransomware encryption become magnified when an organization has failed to prepare.

However, the long-term costs of sustaining cybersecurity compromise may be even greater than what financial accounting numbers can show. This is because the intangible costs of cybersecurity compromise are difficult to measure. In the eyes of potential future consumers, any reputational damage involving poor cyber hygiene in the past may deter future business revenue. In a rapidly changing and competitive business world, the ability of a corporation to protect consumer's personal information and maintain the trust of end-users will only become more important in the future.

Business Impact Analysis

Overview

This Business Impact Analysis (BIA) is developed as part of the contingency planning process for the MGM Resorts online booking system. It was prepared on December 2nd, 2021.

Purpose

The purpose of the BIA is to identify and prioritize system components by correlating them to the mission/business process(es) the system supports, and using this information to characterize the impact on the process(es) if the system were unavailable.

The BIA is composed of the following three steps:

1. **Determine mission/business processes and recovery criticality.** Mission/business processes supported by the system are identified and the impact of a system disruption to those processes is determined along with outage impacts and estimated downtime. The downtime should reflect the maximum that an organization can tolerate while still maintaining the mission.
2. **Identify resource requirements.** Realistic recovery efforts require a thorough evaluation of the resources required to resume mission/business processes and related interdependencies as quickly as possible. Examples of resources that should be identified include facilities, personnel, equipment, software, data files, system components, and vital records.

3. **Identify recovery priorities for system resources.** Based upon the results from the previous activities, system resources can more clearly be linked to critical mission/business processes. Priority levels can be established for sequencing recovery activities and resources.

This document is used to build the MGM Resorts Information System Contingency Plan (ISCP) and is included as a key component of the ISCP. It also may be used to support the development of other contingency plans associated with the system, including, but not limited to, the Disaster Recovery Plan (DRP) or Cyber Incident Response Plan.

System Description

The MGM Resorts system architecture consists of routers, network cards, cables, hubs, bridges, switches, modems, web servers, and several storage database servers. The web server uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests all over the world. The databases house customer information regarding bookings and loyalty history as well as general hotel tracking such as room availability, events, and rates. All of the database information is stored on various storage XR2s running proprietary software, encrypted in a redundant fashion on a separate server rack, and is only directly accessible from an internal network. Our hardware is stored in a multi-factor secured room that is under 24/7 video surveillance in our Las Vegas headquarters (3260 Industrial Rd, Las Vegas, NV 89109, USA). We are powered by two separate power companies to ensure consistent availability and have various USPs (universal power supplies).

BIA Data Collection

Through detailed data collection from individual and group interviews, workshops, and questionnaires, the MGM Resorts team offered insight as to critical business functions, essential hardware and staff, and scope of third-party involvement. From the CEO to the Software Engineers to the Front Desk Manager, it is important to have experienced personnel insight to make sure your plan is practical.

Determine Process and System Criticality

Step one of the BIA process – Working with input from users, managers, mission/business process owners, and other internal or external points of contact (POC), identify the specific mission/business processes that depend on or support the information system.

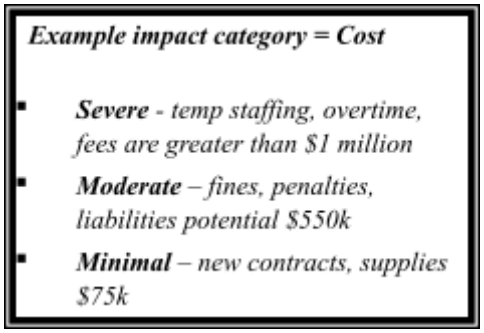
Mission/Business Process	Description
Pay vendor invoice (for hotel costs such as power and water bill)	Process of obligating funds, issuing check or electronic payment and acknowledging receipt (for electrical power, software licensing, internet real estate, etc.)
Customer accessing the website resort booking system	Process of ensuring the website is accessible, reflecting accurate information, and is secure
Web server accessing the database server to determine if a room is available and current rates	Process of making sure the web server and database are running and communicating accurately and in a timely fashion
Room booking and amenity processing and tracking for the resort reservations	Process of ensuring the integrity of the information in the databases and delivering the appropriate confirmation information back to the customer

Identify Outage Impacts and Estimated Downtime

Outage Impacts

Impact categories and values characterize levels of severity to the organization that would result for that particular impact category if the mission/business process could not be performed.

The following impact categories represent important areas for consideration in the event of a disruption or impact.



Impact category: Loss of Revenue

Impact values for assessing category impact:

- Severe = $250,001 and above
- Moderate = $50,001-250,000
- Minimal = $50,000 and below

Impact category: Legal/Regulatory Requirements

Impact values for assessing category impact:

- Severe = Fines and legal fees resulting in greater than $500,000
- Moderate = Fines and legal fees resulting between $50,001-$499,999
- Minimal = Fines and legal fees resulting in less than $50,000

Impact category: Brand, Image, Reputation

Impact values for assessing category impact:

- Severe = In the headlines, greater than 100 negative reviews regarding the incident
- Moderate = Some reports, between 50-99 negative reviews regarding the incident
- Minimal = No news coverage and not public knowledge, fewer than 50 unhappy customers regarding the incident

---

Impact category: Increased Operating Expenses

Impact values for assessing category impact:

- Severe = $250,001 and above
- Moderate = $50,001-250,000
- Minimal = $50,000 and below

The table below summarizes the impact on each mission/business process if MGM

Resorts were unavailable, based on the following criteria:

Individual impact score
- Severe = 7
- Moderate = 3
- Minimal = 1

Overall impact score
- Severe = 18-28
- Moderate = 11-17
- Minimal = 4-10

Mission/Business Process	Impact Category				
	Loss of Revenue	Legal/ Regulatory Requirements	Brand, Image, Reputation	Increased Operating Expenses	Impact (out of 28)
Pay vendor invoice (for hotel costs such as power and water bill)	Minimal	Moderate	Minimal	Moderate	Minimal (8)
Customer accessing the website resort booking system	Severe	Minimal	Severe	Moderate	Severe (18)
Web server accessing the database server to determine if a room is available and current rates	Severe	Moderate	Severe	Moderate	Severe (20)
Room booking and amenity processing and tracking for the resort reservations	Severe	Minimal	Severe	Moderate	Severe (18)

Estimated Downtime

Working directly with mission/business process owners, departmental staff, managers, and other stakeholders, estimate the downtime factors for consideration as a result of a disruptive event.

- **Maximum Tolerable Downtime (MTD).** The MTD represents the total amount of time leaders/managers are willing to accept for a mission/business process outage or disruption and includes all impact considerations. Determining MTD is important because it could leave continuity planners with imprecise direction on (1) selection of an appropriate recovery method, and (2) the depth of detail which will be required when developing recovery procedures, including their scope and content.

- **Recovery Time Objective (RTO).** RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

- **Recovery Point Objective (RPO**). The RPO represents the point in time, prior to a disruption or system outage, to which mission/business process data must be recovered (given the most recent backup copy of the data) after an outage.

The table below identifies the MTD, RTO, and RPO (as applicable) for the organizational mission/business processes that rely on MGM Resorts.

Mission/Business Process	MTD	RTO	RPO
Pay vendor invoice (for hotel costs such as power and water bill)	24 hours	12 hours	12 hours (last backup)
Customer accessing the website resort booking system	2 hours	1 hour	12 hours (last backup)
Web server accessing the database server to determine if a room is available and current rates	2 hours	1 hour	12 hours (last backup)
Room booking and amenity processing and tracking for the resort reservations	4 hours	2 hours	12 hours (last backup)

Maximum tolerable downtime (MTD) is the end all be all of resources being exhausted before your company is increasingly unlikely to recover. Regarding reputation and sales, in the age of the internet, even seconds of interrupted access seem amplified to hours for a user. If someone can't book a room on your site easily, they are likely to stay somewhere else. Recovery time objectives (RTO) help us to understand what kind of recovery and redundancy our systems need in order to recover. Recovery point objectives (RPO) focuses on data loss and the impact that has when recovering and continuing critical business functions. MGM Resorts data is pivotal for accurate booking, rates, room availability, events tracking, and for auditing purposes.

Identify Resource Requirements

The following table identifies the resources that compose MGM Resorts including hardware, software, and other resources such as data files. The assets are listed from most to least important to critical business function.

System Resource/Component	Platform/OS/Version (as applicable)	Description	Dependent CBFs
Web Server x 10	Optiplex GX280	Web Site Host	- Pay vendor invoice (for hotel costs such as power and water bill) - Customer accessing the website resort booking system - Web server accessing the database server to determine if a room is available and current rates - Room booking and amenity processing and tracking for the resort reservations
Database XR2 x 300	Aberdeen storage XR2	Database storage and backup storage	- Web server accessing the database server to determine if a room is available and current rates - Room booking and amenity processing and tracking for the resort reservations
Uninterrupted Power Supply x 60	Tripp Lite TAA-Compliant 3000Va 2700W Smart On-Line Double Conversion Battery Backup, 2U UPS Rack Mount	Backup power supplies to keep servers and databases online in the event of a power outage	- Customer accessing the website resort booking system - Web server accessing the database server to determine if a room is available and current rates - Room booking and amenity

			processing and tracking for the resort reservations
Switch x 10	NETGEAR 20-Port Gigabit Ethernet Unmanaged PoE Switch	Connection for internal network	- Customer accessing the website resort booking system - Web server accessing the database server to determine if a room is available and current rates
Router x 5	TP-Link WiFi 6 Router AX1800 Smart WiFi Router (Archer AX21) – Dual Band Gigabit Router	Connects two or more packet-switched networks or subnetworks	- Customer accessing the website resort booking system - Web server accessing the database server to determine if a room is available and current rates - Room booking and amenity processing and tracking for the resort reservations

It is assumed that all identified resources support the mission/business processes identified in Section 3.1 unless otherwise stated. Please find all additional information in our SSP.

Identify Recovery Priorities for System Resources

The table below lists the order of recovery for MGM Resort resources. The table also identifies the expected time for recovering the resource following a “worst case” (complete rebuild/repair or replacement) disruption.

- **Recovery Time Objective (RTO)** - RTO defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD. Determining the information system resource RTO is important for selecting appropriate technologies that are best suited for meeting the MTD.

Priority	System Resource/Component	Recovery Time Objective
Database XR2's	Aberdeen storage XR2	1 hour
Web Server	Optiplex GX280	1 hour
Router	TP-Link WiFi 6 Router AX1800 Smart WiFi Router (Archer AX21) – Dual Band Gigabit Router	5 hours
Switch	NETGEAR 20-Port Gigabit Ethernet Unmanaged PoE Switch	24 hours
Universal Power Supply	Tripp Lite TAA-Compliant 3000Va 2700W Smart On-Line Double Conversion Battery Backup, 2U UPS Rack Mount	48 hours

Alternative strategies to meet expected RTOs include utilizing our backup equipment, contacting vendor support, and out-sourcing to third-party sellers/data supporters.

Business Continuity Plan

VERSION HISTORY				
VERSION	**APPROVED BY**	**REVISION DATE**	**DESCRIPTION OF CHANGE**	**AUTHOR**
2021-A	Scott Wessel	6/30/2021	New business continuity procedures incorporate cloud technology	Branden Newman
2021-B	Scott Wessel	12/03/2021	Personnel changes	Branden Newman

PREPARED BY	High Five, Inc.	**TITLE**	Risk Management Consultants	**DATE**	12/03/2021
APPROVED BY	Scott Wessel	**TITLE**	Chief Information Officer	**DATE**	12/04/2021

Outline

- Preliminary Confidentiality Statement
- BCP Policy and Objectives
- Scope and Planning Assumptions
- Disaster Declaration Levels and Criteria
- Business Continuity Resource Requirements
- Appendix A – Disaster Recovery
- Appendix B – Team Contacts

Preliminary Confidentiality Statement

The MGM Grand Casinos BCP should be strictly controlled. MGM Grand Casinos data includes private personnel data, proprietary methods, and marketing information. The information in this plan is distributed only to MGM Grand Casinos personnel with a "need to know" and with the understanding that they will hold this information

confidential and will not disclose any information in this plan to third parties without the prior written consent of Bill Hornbuckle, President and CEO, or the filing by the third party of a binding non-disclosure statement that has been vetted by the legal department

Business Continuity Program Policy

The MGM Grand business continuity plan (BCP) ensures that the businesses can continue or immediately resume performing its critical business functions, which are the functions that support the organization's mission, comply with legal requirements, and support life-safety, under all circumstances. This includes natural, technological, and man-made incidents, as well as incidents that result in loss of access to parts of or an entire facility or loss of service due to equipment or systems failure. The benefit of BCP includes the ability to anticipate response actions following a myriad of incidents, improve the business performance of its critical business functions, and ensure timely recovery.

Plan Objectives

The MGM Grand Business Continuity Plan objective is to facilitate the resumption of critical operations, functions, and technology in a timely and organized manner to ensure a viable and stable organization. In doing this it is critical to ensure the safety and well-being of employees, customers, and guests.

The primary objectives of the plan are to:

- Maintain Critical Business Functions
- Most critical departments/business functions

- Ensure employees can access an alternate facility
- Ensure that employees have safe access to facility
- Protect vital records, ensuring that they are accessible under all conditions
- To document the critical information required for implementation of the Business Continuity Plan.
- To provide guidelines for the MGM Grand for a major disaster that will result in the execution of this Business Continuity Plan.
- To return to near normal operations within 72 hours after a significant disaster event.
- To ensure the Call Center remains operational even if headquarters is closed.
- To maintain a minimal level of customer service 24 X 7.

Once the safety and security of all individuals have been established, MGM Grand defines business continuity as maintaining a level of business function that has an appearance of normalcy. The goal is to stand up alternative resources and methods so that the situation or outage has minimum impact on and visibility to our paying customers, suppliers, vendors, contractors and employees that rely on them, all while maintaining compliance with General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA), and the Payment Card Industry Data Security Standard (PCI DSS) regulations. Meanwhile the BCP is to remain in effect until the disaster recovery procedures have restored critical resources to pre-event levels or as close to it as possible. MGM Grand's organizational-wide business continuity plan will be developed under the supervision of Branden Newman, the Chief Information Security

Officer and acting BCP Lead. He will report to Scott Wessel, the CIO of MGM Grand. Mr. Wessel will in turn provide timely updates to the president and CEO Bill Hombuckle.

Scope and Planning Assumptions

Scope -

The scope of this plan covers: MGM Grand Casinos 3799 S Las Vegas Blvd, Las Vegas, NV 89109

The plan is applicable once the life and safety of employees, customers, and guests has been verified and in the event that a facility is or will become inaccessible. It can be active during normal business hours and after hours, with and without warning.

Assumptions -

The following assumptions were used while creating this plan:

- That a worst-case scenario the MGM Grand Casinos point of sales web servers located at 3799 S Las Vegas Blvd, Las Vegas, NV 89109 which services all MGM Grand casinos throughout the continental U.S. and around the world are unavailable for the extended period of time of 72 hours.
- That a backup of critical computer systems occurs daily (usually around midnight) and these backups (usually tape) are sent to offsite storage early the next morning.
- That MGM Grand maintains an Emergency Operations Center (EOC) here on premise. However, if the situation warrants building evacuation, the EOC is

located at the Bellagio Hotels at 3600 S Las Vegas Blvd, Las Vegas, NV 89109. All managerial meetings will occur at the EOC.

- That a car service has been contracted to pick up management at any time of the day for transport to the EOC.
- That management will approve increases to the limit of Team Leads corporate credit cards to facilitate procurement of equipment and supplies.
- That furnishing, equipment, and supplies can be readily obtained from current vendors.
- That the level of the BCP detail is based on the premise that sufficient and knowledgeable Company personnel will not be incapacitated by the interrupting event, and can execute the Business Continuity Plan.

Disaster Declaration Levels and Criteria

	Severity Level	Criteria	Actions
Disaster Management	Disaster 24hrs – Up	• Severe impact to several critical databases resulting in the **inability of web server to provide critical functions**, processes or services, mainly reservation booking • Outage expected to exceed the RTO (24 hrs) to resolve	• Immediately escalate through Executive Leadership and **Declare** (activate BCP) • **Mobilize recovery teams** and begin recovery process • **Activate business continuity plans** (workaround procedures for critical processes dependent on database)

	Crisis 3-24hrs	• Moderate to severe impact to one or more critical databases that has the potential to prevent the web server from providing critical functions, processes or services, mainly reservation booking if not restored within 24 hrs • Outage may or may not exceed the RTO (24 hrs) to resolve • Potential to replace damaged equipment or restore data locally within RTO (12 hrs)	• Assess damage to determine the extent of the disruption • Decide if business continuity plans should be activated • If outage is expected to exceed OTC RTO (24 hrs) or if the impact expands to additional critical systems, **escalate to Disaster** otherwise address via incident management
Incident	Critical 0-3hrs	• An issue is considered 'Critical' when Business critical applications are impacted, regardless of the cause	• Disaster Management Team immediately communicates incident to users and other affected parties via email. • Provide hourly status updates • If outage is expected to exceed target resolution time for critical incidents (1 business day), **escalate to Crisis**
	High	• While not as serious as a critical issue, high impact issues causing a major disruption in providing service to the business requiring immediate attention	• DMT immediately communicates incident to users and other affected parties via email. • Provide regular status updates

Business Continuity Resource Requirements

Resource Category	Resource Details	Normal Quantity	Quantity Needed Following Disaster			
			24 hours	72 hours	1 week	Later (specify)
Managers						Migrate to AWS
Staff	CSR, Reservation Operators	10	75	50	25	
Office Space	Cold, Warm, Hot Site		Hot Site x 1	Warm Site x 1	Cold Site x 1	
War Room	For Managers, CIRT,					
Data center	Backup Data Center					
Vital records, data, information	Hard Drive and Tape Backups					
Vital Equipment	Web Server	Server x 10	Server x 4	Server x 2	Server x 2	
Vital Equipment	Database Server	Server x 10	Server x 4	Server x 2	Server x 2	
Vital Equipment	Firewall/Router	Router x 4	Router x 2	Router x 2	Router x 1	
Vital Equipment	Switch	Router x 4	Router x 2	Router x 2	Router x 1	
Office Equipment	Uninterrupted Power Supply		4	2	2	
Vendor/Contractor	Hotels.com, Expedia.com, Travelosity.com	Handle 15% of Reservations	Handle 30% of Reservations	Handle 60% of Reservations	Handle 90% of Reservations	

Appendix A - Disaster Recovery

Below is a snapshot of the data center disaster recovery checklist. Download and print the full comprehensive checklist from https://www.allbusinesstemplates.com/template/2KXUZ/data-center-disaster-recovery-plan/ .

	Plan Element	Recommended Action
☐	Data backup	
☐	Power management	
☐	HVAC management	
☐	Utility management	
☐	Initiate application-level backup procedures	
☐	Initiate hardware-level backup procedures	
☐	Initiate network backup procedures	
☐	Initiate security procedures	
☐	Initiate other backup procedures	
☐	Contact third-party organizations	
	Decision to declare disaster	
☐	Can situation be handled without staff leaving building?	
☐	If situation is deemed serious, issue evacuation orders immediately	

A-1 Sequence of Recovery Activities

The following activities occur during recovery of the MGM Grand database:

1. Identify recovery location (if not at original location)
2. Identify required resources to perform recovery procedures
3. Retrieve backup and system installation media.
4. Recover hardware and operating system (if required).

5. Recover system from backup and system installation media.

A-2 Recovery Procedures

The following procedures are provided for recovery of the MGM Grand database at the original or established alternate location. Recovery procedures are outlined per team and should be executed in the sequence presented to maintain an efficient recovery effort.

These procedures are used for recovering a file from backup tapes. The Computer Incident Recovery Team is responsible for reloading all critical files necessary to continue production.

1. Identify file and date from which file is to be recovered.
2. Identify tape numbers using a tape logbook.
3. If tape is not in the tape library, request tape from the recovery facility; fill out with appropriate authorizing signature.
4. When tape is received, log date and time.
5. Place tape into the drive and begin the recovery process.
6. When file is recovered, notify Disaster Management Team Lead

A-3 Validation Data and Functionality Testing

Validation data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely. Validation functionality testing is the process of verifying that recovered MGM Grand database functionality has been tested, and the system is ready to return to normal operations. The following

procedures will be used to determine that the recovered data is complete and current to the last available backup:

1. Have Sr. Database Engineer run query against database to confirm:
    a. Completeness (no blank or null values)
    b. Uniqueness (no duplicate values)
    c. Consistency (data format is as expected)
2. Have Sr. Systems Administrator run PowerShell scripts to test and confirm file and folder permissions are accurate and check system logs.
3. Have Sr. Web Administrator run simulation transactions and check logs.

A-4 Backups

As soon as possible following recovery, the system should be fully backed up and a new copy of the current operating system stored for future recovery efforts. This full backup is then kept with other system backups. The procedures for conducting a full system backup are:

1. Open Object Explorer and expand the server tree.
2. Right-click on the database, go to Tasks...Backup...select OK.
3. Choose the connected SAN device as a destination.
4. Run PowerShell script in task manager to automate steps 1-3.
5. Launch Iron Mountain software and run full backup of step 3 to tape.

Appendix B - Team Contacts

Computer Incident Recovery Team				
NAME	TITLE	PHONE	EMAIL	NOTE
Jonathan Halkyard	Team Lead	702-555-1111		
Ann Hoff	Sr. Database Engineer	702-555-1112		
Tilak Mandadi	Sr. Web Administrator	702-555-1113		
Ron Williams	Sr. Systems Administrator	702-555-1114		
DISASTER MANAGEMENT TEAM				
NAME	TITLE	PHONE	EMAIL	NOTE
Branden Newman	Team Lead	702-555-1115		
Laura Lee	Sr. Project Manager	702-555-1116		
Ricky Bobby	Sr. Project Manager	702-555-1117		
Ron Williams	Sr. Regional Manager	702-555-1118		
VENDORS				
NAME	TITLE	PHONE	EMAIL	NOTE
Travelosity.com				
Expedia.com				
Hotels.com				
Orbitz				
VENDORS (CONT.)				
NAME	TITLE	PHONE	EMAIL	NOTE
Las Vegas Temp Staffing		702-555-1318		
Amazon Web Services		702-555-2518		
Cloudflare		702-555-3138		
Iron Mountain		702-555-4118		
SENIOR MANAGEMENT				
NAME	TITLE	PHONE	EMAIL	NOTE
Bill Hombuckle	CEO, MGM GRAND			
Scott Wessel	CIO, MGM GRAND			

References

Ackerly, Rachel. “The Cost of Ransomware Attacks: Why and How You Should Protect Your Data.” *Cisco Umbrella*, 16 Aug. 2021, https://umbrella.cisco.com/blog/cost-of-ransomware-attacks.

AllBusinessTemplates.com, “n.d.”, Data Center Disaster Recovery Plan Example https://www.allbusinesstemplates.com/download/?filecode=F3REJ&lang=en&iuid=5a1d16f6-0994-4615-9315-c1462e67613e

Bhatia, P. (2021). *A summary of 10 key GDPR requirements*. EUGDPR Academy. Retrieved October 11, 2021, from https://advisera.com/eugdpracademy/knowledgebase/a-summary-of-10-key-gdpr-requirements/

Chron, C. (05/28/2020) “Responsibilities of an Information System Security Officer” https://work.chron.com/responsibilities-information-system-security-officer-15533.html

Cloudflare. “Cloudflare Ddos Protection & Mitigation.” *Cloudflare*, https://www.cloudflare.com/ddos/.

Coble, Sarah. “Equifax Pays Indiana $19.5m to Settle Data Breach Case.” *Infosecurity Magazine*, 16 Apr. 2020, https://www.infosecurity-magazine.com/news/equifax-pays-indiana-195m/.

Coble, Sarah. “Orbitz and Expedia Agree to Data Breach Settlement with Pennsylvania.” *Infosecurity Magazine*, 16 Dec. 2019, https://www.infosecurity-magazine.com/news/orbitz-and-expedia-agree-data/.

Data Security and Natural Disasters.” *Idx.us*, https://www.idx.us/knowledge-center/data-security-and-natural-disasters.

DisasterRecoveryPro, 2020. What is a Business Impact Analysis?. [online] Youtube.com. Available at: <https://www.youtube.com/watch?v=hY31GhZBga8&t=7s>.

Exabeam. (2021). *PCI Security: 7 Steps to Becoming PCI Compliant*. Exabeam. Retrieved October 09, 2021, from https://www.exabeam.com/information-security/pci-security-7-steps-to-becoming-pci-compliant/“

Gibson, Darril. *Managing Risk in Information Systems.* Third Edition. “Chapter 11 - Turning a Risk Assessment into a Risk Mitigation Plan.” Slide 45.

Gilbert, A. (2021, August 19). *California Consumer Privacy Act (CCPA) compliance guide: Everything you need to know*. Osano. Retrieved October 09, 2021, from https://www.osano.com/articles/ccpa-guide

Idx.us. “Data Security and Natural Disasters.” *Idx.us*, https://www.idx.us/knowledge-center/data-security-and-natural-disasters.

Inspirien.net (April 7, 2020), Business Continuity Plan Montgomery, AL https://www.inspirien.net/wp-content/uploads/2020/04/Inspirien-Business-Continuity-Plan.pdf

McDonald, Andy (October 24, 2021), Simple Data Validation in SQL https://sqlspreads.com/blog/simple-data-validation-in-sql/

MGM Resorts. “Frequently Asked Questions.” *MGM Resorts,* https://www.mgmresorts.com/en/faq.html.

NIST, n.d. NIST Business Impact Analysis (BIA) Template (word). [online] csrc.nist.gov. Available at: <https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FPublications%2Fsp%2F800-34%2Frev-1%2Ffinal%2Fdocuments%2Fsp800-34-rev1_bia_template.docx&wdOrigin=BROWSELINK>.

NIST.gov, “n.d.”, NIST SP 800-53 Security Controls from the Contingency Planning Family https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fcsrc.nist.gov%2FCSRC%2Fmedia%2FPublications%2Fsp%2F800-34%2Frev-1%2Ffinal%2Fdocuments%2Fsp800-34-rev1_cp_template_high_impact_system.docx&wdOrigin=BROWSELINK

Ready.gov, “n.d.”, Business Continuity Resource Requirements https://www.ready.gov/sites/default/files/2020-03/business-continuity-resource-worksheet.pdf

RiskSOURCE Clark-Theders, 2014. Business Impact Analysis. [online] Risksource.com. Available at: <https://risksource.com/wp-content/uploads/2018/06/Sample-Business-Continuity-Plan-Template.pdf>.

RCN Business, 2021. What Is A Business Impact Analysis? (And How To Get Started) | RCN Business. [online] Rcn.com. Available at: <https://www.rcn.com/business/insights-and-news/insights-articles/business-impact-analysis/>.

Smartsheet, “n.d.” Business Continuity Program Template (Word) https://view.officeapps.live.com/op/view.aspx?src=https%3A%2F%2Fwww.smartsheet.com%2Fsites%2Fdefault%2Ffiles%2FIC-Business-Continuity-Program-9465_WORD.dotx&wdOrigin=BROWSELINK

Stevens, M. (11/17/2016).”Analyzing The CIO's Roles & Responsibilities Regarding Cybersecurity” https://www.bitsight.com/blog/analyzing-cios-roles-responsibilities-cybersecurity

Tech Target, 2008. Business impact analysis for business continuity: Data collection methodologies. [online] SearchITChannel. Available at: <https://searchitchannel.techtarget.com/feature/Business-impact-analysis-for-business-continuity-Data-collection-methodologies>.

Verizon 2020 Data Breach Investigations Report (DBIR), 22% of data breaches involve phishing. “50 Phishing Stats You Should Know in 2021.” *Expert Insights*, 26 Oct. 2021, https://expertinsights.com/insights/50-phishing-stats-you-should-know/.

Whitman, M. E., Mattord, H. J., & Green, A. (2014). *Principles of Incident Response and Disaster Recovery* (Second Edition ed.). Cenegage Learning.