Flo-Motion Games: IT Security Assement

Charles Kanakan

Vulnerability assessment plan

- Asset List and Valuation
  - Physical assets
    - Office space
    - Office materials
    - Intellectual properties (IPs)
    - Distribution
      - Warehouse employees
      - Storage
      - Delivery
  - Human assets
    - Game programmers
    - Game designers
    - Marketing team
    - Accountants
  - Information Technology assets
    - Hardware
      - Laptops
      - Cameras
      - Motion Capture technology
      - Tablets
    - Software
      - Unreal engine
      - MT Framework
      - Havoc engine
      - Unity
      - Game Maker studio
      - Photoshop
    - Data
      - Video game program backups

- Database for employee information
- Customer Information
- Sales Information
- Inventory

- Threat identification
  - All possible threats
    - Threats for Hardware
    - Threats for Software
    - Physical threats
- Vulnerability
  - Testing for vulnerabilities
  - The possibility and damages of each risk
  - Overall risk assessment
- Risk Mitigation
  - Acceptable amount of loss
  - Monitoring problem areas
  - Determining best course of action

Security Policy

- Summary of security policy
  - Policy on equipment
  - Policy on software
  - Interaction with outside companies
  - Database access
  - Use of websites
  - Hardware removal
- Employee access Policy
  - Level of access
  - Policy on outside technology

        - Use of company technology
    - Physical security policy
        - Getting into the building
        - Security personnel
        - Termination of employee
        - Protocol for dealing with dangerous people
            - Training
            - When someone has a weapon
    - Enforcement
        - List of violations
        - Potential dangers of not following policy

Business Continuity plan

- The reason for creating a business continuity plan
- A team that identifies potential dangers
- Its purpose and responsibilities
- Determining resources that could become compromised
- Introducing plans to solve problems
- Training employees
- Creating groups
    - Constant practice on procedure
    - Document
        - Detailing the procedure
- Create a recovery plan

Product Acquisition Plan

- Hardware
- Software

Vulnerability Assessment

Assets

Physical Assets

Assets	Description
Office space	Workspace.
Office materials	The material used for work.
Intellectual properties	The games we create and own.
Distribution	This includes warehouse employees, storage, and companies we distribute.

Human Assets Tables

Asset	Responsibility
Game Programmers	They program each video game we make
Game Designers	The designer of the story, structure, and mechanics of the game
Marketing team	Marketing our video games.
Accountants	The management of money.

Information Technology assets

Hardware assets

Asset	Description
Laptops	Issued to every employee for work purposes.
Cameras	Used for security purposes. Monitoring of the work environment.

Motion capture technology	Used to capture for real-life body animation for video games
Tablets	Used for accounting purposes

Software assets

Asset	Description
Unreal engine	Game programming language for 3D games.
MT Framework	Game programming language for 3D games.
Havoc engine	A physics engine used in video games.
Unity 3D	Game programming language for 2D and 3D games.
Game Maker studio	Game programming language for basic 2D games.
Photoshop	Used to create and alter art for our games.

Data

Below is the data that we are keeping track of.

Video game program backups: We have backups of all the games we make

Database for employee information: This includes personal information, salary and job position of every employee.

Sales Information: The information of our transactions with customers and companies that buy our products.

Inventory: A detailed report on our storage and the company we distribute to.

Threat evaluation

Threats to Hardware:

Type of threat	Example
Natural disasters	Floods, hurricanes, fires, earthquakes, etc.
Disgruntled employees	Angry employees destroying hardware.
Power outages	Power going out and destroying our hardware.
Hardware failure	Hardware not working.
Out of date hardware	Hardware that has become obsolete.

Threats to software

Type of threat	Example
Pirating	People creating illegal copy of our games.
Disgruntled employees	Employees selling information about our games or compromising our software.
Hacking	Someone hacking into our system and comprising it.
Malware and viruses	Malware and viruses infecting our system
Network failure	Network servers falling so work cannot be done.
Software failure/termination	Software failure or using software that is no longer being supported.

Physical threats

Type of threat	Example
Vandalism	Someone destroying company properties
Disgruntled employees	An angry employee looking to do physical harm to someone.
Angry costumers	Customers who are unhappy with our products and looking to inflict harm.

Vulnerability

This is how we will test vulnerabilities

Type of tests	Purpose
Penetration testing	To find possible holes in our system.
White hat hacking	Hiring a hacker to find exploits.
Malware scans	Scanning for potential malware in our system.

The possibility and damages of each risk.

Below is a table of the risks I deem most important.

Threat	Possibility	Impact	Potential loss
Natural disasters	High	High	$500,000
Hacking	High	High	$35,000
Loss of hardware: Laptops and tablets	High	High	$15,000
Malware and viruses	Mid	High	$20,000

Pirating	Mid	Mid	$40,000
Power outages	Low	Mid	$30,000
Disgruntled employees	Low	High	$30,000
Network failure	Low	Low	$5,000

Risk mitigation table

Threat	Risk mitigation	Reason
Natural disasters	A warm site to continue working.	If our office space is destroyed in a disaster. There will be a backup site with functioning network servers and ample space to work.

Hacking	Backups of our data on hard-drive and flash drives.	To have backups of our data and do not have to adhere to hackers.
Malware and viruses	Installing anti-virus software	We need protection from malware and viruses. We risk being compromised.
Pirating	Nothing	We trust our profits on our games will outweigh the loss in pirated games.
Power outages	Nothing	We will be working on laptops and tablets. So work can continue.
Disgruntled employees	Nothing	There is few ways to anticipate this. In each case, the security officers will handle the situation.
Network server failure	Backup servers to continue working.	If our servers are compromised or not working. We can have backup servers to continue working.

This is the acceptable amount of loss table

Subject	Cost
Office Space	$23,000
Data loss	$3,900
Hardware	$25,000

Monitoring: We will run all of our systems through a bi-weekly security check.

The policy for determining the best course of action is as followed: The severity of damages will dictate whether we deal with the problem.

Security Policy

Summary of Security:

I have detailed security policies for our company to follow. The ACME security policy is to insure the safety of the company and its employees. This policy covers equipment, software, and physical security. As well as the punishment for not following procedure.

Policy on equipment

Subject	Policy
Equipment	Office equipment must to be used for work purposes.
Software	No outside software can be used on company equipment.
Database Access	Job position will determine what parts of our database an employee has access to.
Use of websites	There will be web filters blocking certain websites.
Hardware removal	All information on the hardware.

Employee Access Policy

Subject	Policy
Level of access	Job status and years working at the company will determine what a person has access to. E.g.

	Seeing code, level design documents
Policy on outside technology	**Personal computers:** Must have anti-virus software downloaded. **Phones:** Employees can use their own phones. Flash drives and external hard-drives: Must have
Dealing with outside companies	Outside company employees will not have access to
Use of company technology	All technology owned by the company must only be used for business-specific purposes.

Physical security policy

Subject	Policy
Getting into the building	Each employee will have a card key and passcode to access the building.
Security personnel	There will be at least two security officers in building. They must adhere to the same rules as the other employees.
Termination of employee	A security officer will escort terminated to gather their belongings.
Dealing with dangerous people	When there is a dangerous person on the premises. Call security or the police. Do not engage them.

Enforcement

List of Violations

Violations	Description	Repercussion

Harassment	Constantly insulting, hazing, undermining fellow employees	Possible suspension or termination.
Physical harm	Any physical contact met to do harm.	Immediate termination
Tempering with software	Unauthorized changes to video game code.	Possible suspension
Leaking information about our products	Leaking classified information on games. It includes code, mechanics, structure, story details.	Dependent of the severity of the information the employee may face suspension or termination.
Stealing equipment	Stealing company equipment	Week-long suspension or possible termination

Failure to follow the security policies can potentially put the company and personal information and livelihood at risk. The repercussions are based severity. As well as amount of offences.

Business Continuity plan

The purpose of creating a business continuity plan to allow us to continue working even in case of disaster. There will be a team comprised of ten people to carry out the business continuity plan.

Team: Will identify potential dangers to the company. They will meet every month to go over. They will be comprised of three high level executives and seven employees selected from various departments.

Responsibilities: The team is responsible for putting our company in a position to continue working after a disaster happens. They will determine whether resources have been compromised. They will run monthly test for the most likely risk.

Plans: Step-by-step plans on how the company will deal with each risk.

Training: The team will conduct training sessions twice a year on the procedure. All employees will be present. Employees will be given a document on procedure.

Creating a recovery plan: First, the team will determine the worst possible outcomes for each risk. Then they will determine bare minimum hardware and software. That is needed to proceed with work. The team will take 5-6 additional employees to conduct full recovery. Restoring network server will be the first priority. The intended timetable for recovery is a month.

Product Acquisition Plan

- Hardware- That we need to acquire.

Name	Purpose	Reason	Cost
Lepin flash drive	Backup storage	Out of the flash drives I researched, this has satisfactory security and is affordable.	$37.99

- Software- That we need to acquire.

Name	Purpose	Reason	Cost
Wireshark	Monitoring network server activity	Has data filtering, packet sniffing and multiple IP address packet capture. Has similar features to other packet analyzers.	Free
Comodo Internet Security Firewall	A firewall to protect from unauthorized access	Multi-layered protection, Impact assessment.	Free

Sticky Password premium	For password security	Has unlimited storage, two factor identification.	Free
SolarWinds Event & Log Manager	For gathering data to predict potential attacks.	Constantly learns from past mistakes. Instantly identifies attacks.	$4,495
Avast Free Antivirus 2017	Providing protection from malware and viruses.	It has many features that other anti-virus software have. Some features are Malware protection, Wi-Fi inspector, and simple password manager	Free
Prey	For finding lost Android phones and iPhones. Also	Allows for remote lockout and deletion.	Free

References

Aegis Secure Key - USB 3.0 Flash Drive. (n.d.). Retrieved April 29, 2018, from https://www.apricorn.com/aegis-secure-key-3

Business Continuity Planning. (n.d.). Retrieved February 25, 2018, from https://www.aberdeenshire.gov.uk/business/support-and-advice/business-support/Business-Continuity-Planning/

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). *INFORMATION SECURITY POLICY COMPLIANCE: AN EMPIRICAL STUDY OF RATIONALITY-BASED BELIEFS AND INFORMATION SECURITY AWARENESS*. MIS Quarterly, 34(3), 523-A7.

Capsa Network Analyzer. (n.d.). Retrieved April 15, 2018, from https://www.colasoft.com/capsa/

Cisco ASA 5500-X Series with FirePOWER Services. (2018, February 15). Retrieved February 25, 2018, from https://www.cisco.com/c/en/us/products/security/asa-firepower-services/index.html#~stickynav=2

Comodo Internet Security. (n.d.). Retrieved February 25, 2018, from https://help.comodo.com/topic-72-1-451-4685-.html

Comparison of USB flash drives with Encryption & Biometrics. (n.d.). Retrieved April 29, 2018, from https://www.rohos.com/knowledge-base/comparison-of-encryption-biometric-usb-drives/

Compare Kiwi Syslog to SolarWinds Log & Event Manager. (n.d.). Retrieved February 26, 2018, from https://www.kiwisyslog.com/compare-kiwi-syslog-solarwinds-log-event-manager

Completed Product sample (2013, May 8). *Assessment of the current IT infrastructure*. Retrieved from:https://curry.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_30110_1&content_id=_661495_1&mode=reset

ConsumersAdvocate (n.d.). *Get Your Sticky Password Premium License for a super price*. Retrieved April 09, 2018, from: https://www.stickypassword.com/lp/consumersadvocate?utm_source=consumersadvocate2017&utm_medium=promo&utm_term=pli&utm_content=lpl50&utm_campaign=2017-10_consumersadvocate&campaign_affid=d-adprac-1186-lp50

Find My iPhone on the App Store. (2010, June 18). Retrieved from: https://itunes.apple.com/us/app/find-my-iphone/id376101648?mt=8

Inc. (2011, November 01). *Prey Find my Phone Tracker GPS on the App Store*. Retrieved from https://itunes.apple.com/us/app/prey-find-my-phone-tracker-gps/id456755037?mt=8

Hindy, J. (2018, March 12). *5 best find my phone apps and other find my phone methods too!* Retrieved from: https://www.androidauthority.com/best-find-my-phone-apps-for-android-and-other-find-my-phone-methods-too-565016/

Jović, F. (n.d.). EventLog Analyzer. Retrieved February 26, 2018, from https://www.netvizura.com/eventlog-analyzer

KANGURU Hardware Encrypted Secure Flash Drive 128GB USB 3.0 USB Flash Drive Black | Staples. (n.d.). Retrieved April 29, 2018, from https://www.staples.com/kanguru-hardware-encrypted-secure-flash-drive-128gb-usb-3-0-usb-flash-drive-black/product_IM1UZ9555

Kirvan, P. (2012, July). *Comparing the costs of hot sites and cold sites.* Retrieved May 1, 2018, from https://searchdisasterrecovery.techtarget.com/answer/Comparing-the-costs-of-hot-sites-and-cold-sites

LastPass Free features. (n.d.). Retrieved April 08, 2018, from https://lastpass.com/features_free.php

Lepin Flash Drive Military Grade. (n.d.). Retrieved April 29, 2018, Retrieved from: https://www.amazon.com/lepin-Military-AES-CBC-Encrypted-Advanced/

LOGalyze. (n.d.). Retrieved February 26, 2018, from http://www.logalyze.com/

Log & Event Manager. (n.d.). Retrieved February 26, 2018, from https://www.solarwinds.com/log-event-manager-software

Microsoft Message Analyzer Operating Guide - Message Analyzer. (n.d.). Retrieved April 15, 2018, from https://docs.microsoft.com/en-us/message-analyzer/microsoft-message-analyzer-operating-guide

RoboForm Password Manager. (n.d.). Retrieved April 08, 2018, from https://www.roboform.com/?gclid=EAIaIQobChMI6vv0mOer2gIVyVuGCh0F9QTHEAAYAyAAEgJZiPD_BwE

Rubenking, N. J. (2017, February 23). *Avast Free Antivirus 2017*. Retrieved from https://www.pcmag.com/article2/0,2817,2471522,00.asp

Rubenking, N. J. (2017, October 12). *Symantec Norton AntiVirus Basic*. Retrieved from https://www.pcmag.com/article2/0,2817,2424097,00.asp

Rubenking, N. J. (2017, September 22). *McAfee AntiVirus Plus*. Retrieved from https://www.pcmag.com/article2/0,2817,2469309,00.asp

Rubenking, N. J., Rubenking, N., San Francisco PC User Group, IBM, & Association of Shareware Professionals. (2018, March 07). *The Best Antivirus Protection of 2018*. Retrieved from https://www.pcmag.com/article2/0,2817,2372364,00.asp

Rubenking, N. J. (2017, October 12). *Symantec Norton AntiVirus Basic*. Retrieved from https://www.pcmag.com/article2/0,2817,2424097,00.asp

Rubenking, N. J. (2017, October 20). *Webroot SecureAnywhere AntiVirus*. Retrieved from https://www.pcmag.com/article2/0,2817,2470312,00.asp

Smith, D. M. (2017, October 29*). The Cost of Lost Data - A Peer-Reviewed Academic Articles | GBR*. Retrieved May 1, 2018, from https://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/

SonicWall TZ300 Network Security/Firewall Appliance. (n.d.). Retrieved February 25, 2018, from https://www.pcnation.com/web/details/ZL8824/SonicWall-TZ300-Network-Security-Firewall-Appliance-01-SSC-0215-758479002154

Student 1(n.d.) *Student Phase 1 Water Savers Corporation.* Retrieved from: https://curry.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_30110_1&content_id=_661622_1

Student 2 (2012, Apr 2) *Project Phase one.* Retrieved from: https://curry.blackboard.com/webapps/blackboard/content/listContent.jsp?course_id=_30110_1&content_id=_661622_1

The Cost of Hackers in the US [Infographic] | WebpageFX. (2015, July 07). Retrieved May 1, 2018, from https://www.webpagefx.com/data/cost-of-hackers-in-the-us/

The True Cost of Missing Hardware: Protecting Yourself From Theft & Loss. (2017, August 16). Retrieved May 2, 2018, from https://threatsketch.com/hardware-theft-loss/

The 8 Best Encrypted Drives of 2018. (2017, March). Retrieved April 29, 2018, from https://www.fabathome.org/best-encrypted-drive/#best-encrypted-flash-drive

Top 10 Encrypted USB Flash Drives. (n.d.). Retrieved April 29, 2018, from https://recoverit.wondershare.com/flashdrive-recovery/top-10-encrypted-usb-flash-drives.html

What is the Real Cost of Computer Viruses? [Infographic] | WebpageFX. (2018, March 16). Retrieved May 1, 2018, from https://www.webpagefx.com/blog/internet/cost-of-computer-viruses-infographic/

Wireshark. (n.d.). Retrieved April 14, 2018, from https://www.wireshark.org/

Wotton, K. (2016, January 27*). E Source Market Research Reveals That Power Outages Cost Businesses Over $27 Billion Annually; Winter Storm Jonas Makes It Worse*. Retrieved April 23, 2018, from https://www.esource.com/ES-PR-Outages-2016-01/Press-Release/Outages

ZSIDISIN, G. A., Melnyk, S. A., & Ragatz, G. L. (2005). An institutional theory perspective of business continuity planning for purchasing and supply management [Abstract*]. International Journal of Production Research, 43(16), 3401-3420*. Retrieved February 25, 2018, from https://www2.chubb.com/Benelux-NL/_Assets/documents/Chubb_Benelux_Risk_Forum_Article_Business_Continuity_Planning.pdf

9 Game Design Software Tools You should be Using. (2018, Feb 23). Retrieved February 25, 2018, from https://www.gamedesigning.org/career/software/

10 Best Password Manager of 2018. (2017, September 12). Retrieved April 07, 2018, from:

https://www.consumersadvocate.org/password-manager/a/best-password-manager