CST-407 Activity 1 The ABCs of Information Security

Alex M. Frear

College of Science, Engineering, and Technology, Grand Canyon University

Course Number: CST-407

Professor: Dr. Melody White

07/22/2025

Table of Contents

Checkpoint 1 – Understanding the CIA Triad

Problem	C.I.A. Issue(s) Involved	Reason for Your Decision	Source (APA In-Text Citation)
Yahoo	Confidentiality	Hackers exfiltrated user account data (names, DOBs, hashed passwords), exposing sensitive information without authorization.	(Larson, 2017)
Equifax	Confidentiality	Attackers stole Social Security numbers, birth dates, and credit data—unauthorized disclosure of personal financial information.	(Fruhlinger, 2020)
Target	Confidentiality	Malware on POS systems captured credit/debit card details and customer PII—sensitive data was accessed and removed without permission.	(Committee on Commerce, Science, and Transportation, 2014)
NASA's Mars Orbiter	Integrity	A unit-conversion mismatch corrupted navigation data, causing the probe to follow incorrect commands—data was altered and veracity lost.	(NASA, n.d.)
Knight Capital	Integrity	A bad software update activated an obsolete trading module, producing erroneous orders—data/process integrity was corrupted.	(Heusser, 2012)
Colonial Pipeline	Availability	Ransomware shut down fuel pipeline operations, halting service delivery and denying timely access to critical resources.	(Kerner, 2022)
SolarWinds	Confidentiality	Sunburst malware in trusted updates exfiltrated sensitive data from government and corporate networks—unauthorized disclosure of information.	(Government Accountability Office, 2021)
AT&T	Confidentiality	Hackers stole Social Security numbers, account numbers, and passcodes from millions of customers—personal data was viewed and taken without consent.	(Hauari, 2024)
Ticketmaster	Confidentiality	SQL injection attacks exposed order history and payment data for over 560 million users—customer records were copied and leaked.	(Alger, 2024)

CrowdStrike Outage	Availability	A faulty software update crashed servers globally—critical monitoring services became unreachable and disrupted operations.	(Sato, 2024)

Checkpoint 2 – Identification of Motive, Method, and Opportunity (MoM)

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source (APA In-Text Citation)
Motive	Colonial Pipeline	The DarkSide ransomware actors demanded cryptocurrency payment (75 BTC, ≈$5 million) to decrypt Colonial Pipeline's systems—demonstrating a clear financial motivation.	(Reuters, 2021)
Method	Target	Attackers leveraged stolen credentials from an HVAC vendor to breach the data connection used for billing, then uploaded point-of-sale malware onto Target's network.	(Hosenball, 2014)
Opportunity	Equifax	Attackers exploited a website application vulnerability to gain access to files containing personal data—Equifax's failure to secure its web-facing application provided the clear opportunity for the breach.	(Swamynathan, 2017)

Checkpoint 3 – Cybersecurity Response Types

Response Type	Company Involved	Reason for Your Decision	Source (APA In-Text Citation)
Prevention	Target	After the 2013 breach, Target accelerated a $100 million program to deploy chip-enabled smart cards and PIN verification in its stores, proactively hardening payment security to prevent future breaches.	(Reuters, 2014)
Deterrence	Equifax	The 11th U.S. Circuit Court upheld a $380.5 million class-action settlement against Equifax for its 2017 breach, enforcing financial penalties and setting a regulatory precedent to deter similar lapses.	(Reuters, 2021)
Detection	AT&T	In July 2024, AT&T discovered that records for 109 million customer accounts had been illegally downloaded and promptly involved the FBI, demonstrating effective monitoring and incident-detection processes.	(Shepardson, 2024)
Mitigation	Colonial Pipeline	Following the May 2021 ransomware attack, Colonial Pipeline immediately shut down its entire network to contain the threat and prevent further spread of malware across its critical infrastructure.	(Reuters, 2021)
Recovery	CrowdStrike	On July 19, 2024, CrowdStrike deployed a software fix that restored service to millions of impacted Windows hosts worldwide, rapidly reversing the effects of its own faulty update.	(Reuters, 2024)

Checkpoint 4 – Understanding of Data States

Data State	Company Involved	Reason for Your Decision	Source (APA In-Text Citation)
Data at Rest	Equifax	Equifax stored unencrypted Social Security numbers, birth dates, and credit data in its databases. When attackers exfiltrated this repository, they accessed sensitive information “at rest.”	(Fruhlinger, 2020)
Data in Transit	Ticketmaster	During the 2024 breach, SQL-injection attacks targeted data as it moved between Ticketmaster’s web servers and users, intercepting order histories and payment information “in transit.”	(Alger, 2024)
Data in Use	Knight Capital	The Knight Capital incident involved bad code updating active trading algorithms—data loaded in memory was altered, corrupting live trades and demonstrating a compromise of “data in use.”	(Heusser, 2012)

Checkpoint 5 – Application of OWASP Top 10

Vulnerability	Company Involved	Reason for Your Decision	Source (APA In-Text Citation)
Injection	Ticketmaster	The 2024 Ticketmaster breach was executed via an SQL injection vulnerability in its web application, allowing attackers to run unauthorized database queries and steal data for 560 million users.	(Alger, 2024)

References

Alger, C. (2024, June 15). Security leaders respond to Ticketmaster breach. *Security Magazine*. Retrieved from https://www.securitymagazine.com/articles/100743-security-leaders-respond-to-ticketmaster-breach

Cleveland, C. (2017, September 12). Equifax says data of 143 million Americans exposed in breach. *Reuters*. Retrieved from https://www.reuters.com/article/us-equifax-cyber-idUSKCN1BN1HR

Committee on Commerce, Science, and Transportation. (2014). *A "kill chain" analysis of the 2013 Target data breach*. U.S. Senate. Retrieved from https://www.commerce.senate.gov/publications

Fruhlinger, J. (2020, February 14). Equifax data breach FAQ: What happened, who was affected, what was the impact? *CSO*. Retrieved from https://www.csoonline.com/article/3391376/equifax-data-breach-faq.html

Government Accountability Office. (2021). *SolarWinds cyberattack demands significant federal and private-sector response* [Infographic]. Retrieved from https://www.gao.gov

Hauari, H. (2024, March 28). How to know if you were affected by the AT&T data breach and what to do next. *USA Today*. Retrieved from https://www.usatoday.com/story/tech

Heusser, P. (2012, August 2). Software testing lessons learned from Knight Capital fiasco. *CIO*. Retrieved from https://www.cio.com/article/2397332/software-testing-lessons-learned-from-knight-capital-fiasco.html

Hosenball, M. (2014, February 6). Target vendor says hackers breached data link used for billing. *Reuters*. Retrieved from https://www.reuters.com/article/markets/target-vendor-says-hackers-breached-data-link-used-for-billing-idUSL2N0LB1TM

Kerner, S. M. (2022, May 20). Colonial Pipeline hack explained: Everything you need to know. *TechTarget*. Retrieved from https://www.techtarget.com

Larson, S. (2017, January 31). Every single Yahoo account was hacked – 3 billion in all. *CNN Business*. Retrieved from https://money.cnn.com/2017/01/31/technology/yahoo-hack/index.html

NASA. (n.d.). System failure case studies – Lost in translation. *NASA*. Retrieved from https://www.nasa.gov

Reuters. (2014, February 4). Target to accelerate $100 million chip-enabled smart card program: CFO. *Reuters*. Retrieved from https://www.reuters.com/article/us-target-cfo-idUSKBN0LX1I420140204

Reuters. (2019, July 30). Capital One customer data breach rattles investors. *Reuters*. Retrieved from https://www.reuters.com/article/business/capital-one-customer-data-breach-rattles-investors-idUSKCN1UP1LC

Reuters. (2021, May 8). Cyber attack shuts down U.S. fuel pipeline 'jugular'. *Reuters*. Retrieved from https://www.reuters.com/technology/pipeline-hack-shuts-u-s-fuel-pipeline-2021-05-08/

Reuters. (2021, May 13). Colonial Pipeline paid hackers nearly $5 million in ransom. *Reuters*. Retrieved from https://www.reuters.com/business/energy/colonial-pipeline-paid-hackers-nearly-5-mln-ransom-bloomberg-news-2021-05-13/

Reuters. (2021, June 3). Equifax data breach settlement objectors lose appeal. *Reuters*. Retrieved from https://www.reuters.com/article/us-equifax-settlement-idUSKCN2D42PD

Reuters. (2024, July 19). CrowdStrike deploys fix for issue causing global tech outage. *Reuters*. Retrieved from https://www.reuters.com/technology/crowdstrike-deploys-fix-issue-causing-global-tech-outage-2024-07-19/

Sato, D. (2024, July 19). CrowdStrike and Microsoft: All the latest news on the global IT outage. *The Verge*. Retrieved from https://www.theverge.com

Shepardson, D. (2024, July 12). AT&T says data from 109 million U.S. customer accounts illegally downloaded. *Reuters*. Retrieved from https://www.reuters.com/technology/att-says-data-109-million-us-customer-accounts-illegally-downloaded-2024-07-12/

Swamynathan, Y. (2017, September 8). Equifax reveals hack that likely exposed data of 143 million customers. *Reuters*. Retrieved from https://www.reuters.com/article/business/equifax-reveals-hack-that-likely-exposed-data-of-143-million-customers-idUSKCN1BJ1AQ/