The ABCs of Information Security

CST-407 Application Security Foundations

Owen Lindsey,

September 09, 2025

Contents

Checkpoint #1

Problem	C.I.A. Issue(s) Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
1. Yahoo	Confidentiality	The breach exposed personal information such as names, email addresses, and security questions, which violates the confidentiality of their user's data.	Larson, S. (2017, October 3). *Every single Yahoo account was hacked – 3 billion in all*. CNN Business. https://money.cnn.com/2017/10/03/technology/bu breach-3-billion-accounts/index.html
2. Equifax	Confidentiality	Sensitive personal and financial information, including Social Security numbers and credit card details, was stolen.	Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO. https://www.csoonline.com/article/567634/equifax data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
3. Target	Confidentiality	The attackers stole credit and debit card information along with personal details of millions of customers.	United States Senate Committee on Commerce, Science, and Transportation. (2014). *A "Kill Chain" Analysis of the 2013 Target Data Breach*. U.S. Senate. https://www.commerce.senate.gov/services/files/2 12f4-4468-a4e9-18f3a3a4e9bf
4. NASA	Integrity	The loss of the Mars Climate Orbiter was due to a data mismatch between metric and imperial units, which is a failure of data integrity.	NASA. (n.d.). *System Failure Case Studies – Lost in Translation*. https://www.nasa.gov/
5. Knight Capital	Integrity	A software glitch caused by corrupted data led to erroneous trades, which is a failure in data integrity.	Heusser, M. (2012, August 8). *Software testing lessons learned from Knight Capital fiasco*. CIO. https://www.cio.com/article/2393228/software-testing-lessons-learned-from-knight-capital-fiasco.html

Checkpoint #1

Problem	C.I.A. Issue(s) Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
6. Colonial Pipeline	Availability	The ransomware attack forced the shutdown of the pipeline, making it unavailable and affecting fuel supply.	Kerner, S. M. (2022, June 6). *Colonial Pipeline hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/Coloni Pipeline-hack-explained-Everything-you-need-to-know
7. SolarWinds	Integrity	The attackers compromised the software build process to insert malicious code.	U.S. Government Accountability Office. (2021, July 28). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*. https://www.gao.gov/products/gao-21-105558
8. AT&T	Confidentiality	A data breach exposed the personal information of millions of customers.	Hauari, A. (2024, July 12). *How to know if you were affected by the AT&T data breach and what to do next*. USA Today. https://www.usatoday.com/story/tech/2024/07/12/ data-breach-who-affected-what-to-do/74379292007/
9. Ticketmaster	Confidentiality	The data breach involved the theft of customer and credit card information.	Alger, M. (2024, May 31). *Security leaders respond to Ticketmaster breach*. Security Magazine. https://www.securitymagazine.com/articles/10107 security-leaders-respond-to-ticketmaster-breach
10. CrowdStrike	Availability	The faulty software update caused a global outage, making them unavailable for users.	Sato, M. (2024, July 19). *CrowdStrike and Microsoft: All the latest news on the global IT outage*. The Verge. https://www.theverge.com/2024/7/19/24199411/c microsoft-windows-it-outage-bsod-airlines-banks-down

Checkpoint #2

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Motive	Colonial Pipeline	The attackers' primary motive was financial gain, the ransomware attackers demanded a multi-million dollar payment.	Kerner, S. M. (2022, June 6). *Colonial Pipeline hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/Coloni Pipeline-hack-explained-Everything-you-need-to-know
Opportunity	Equifax	Equifax was aware of a critical vulnerability in its system for months but failed to patch it.	Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO. https://www.csoonline.com/article/567634/equifax data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
Method	Ticketmaster	The breach was carried out using SQL injection attacks.	Alger, M. (2024, May 31). *Security leaders respond to Ticketmaster breach*. Security Magazine. https://www.securitymagazine.com/articles/10107 security-leaders-respond-to-ticketmaster-breach

Checkpoint #3

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Prevention	Equifax	The company's failure to apply a known patch for a critical vulnerability shows a lack of prevenative code maintenance.	Fruhlinger, J. (2020, February 12). *Equifax data breach FAQ: What happened, who was affected, what was the impact?* CSO. https://www.csoonline.com/article/567634/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
Deterrence	Colonial Pipeline	The attack shows a failure of deterrence, as attackers were not discouraged from targeting critical infrastructure.	Wood, Z. (2023, April 18). *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2023/04/18/cybersecurity-policy-responses-to-the-colonial-pipeline-ransomware-attack/
Detection	Target	Target's security systems successfully detected the malware, but the company failed to act on the alerts.	Chiacu, D. (2014, March 26). *Target missed many warning signs leading to breach: U.S. Senate report*. Reuters. https://www.reuters.com/article/us-target-breach-senate/target-missed-many-warning-signs-leading-to-breach-u-s-senate-report-idUSBREA2P13920140326
Mitigation	Target	After detection, Target isolated compromised POS systems to contain further spread of malware, showing partial mitigation efforts.	Chiacu, D. (2014, March 26). *Target missed many warning signs leading to breach: U.S. Senate report*. Reuters. https://www.reuters.com/article/us-target-breach-senate/target-missed-many-warning-signs-leading-to-breach-u-s-senate-report-idUSBREA2P13920140326
Recovery	CrowdStrike	The global outage required a massive recovery effort, with companies manually removing the faulty update and airlines taking over a week to restore normal operations.	Sato, M. (2024, July 19). *CrowdStrike and Microsoft: All the latest news on the global IT outage*. The Verge. https://www.theverge.com/2024/7/19/24199411/crowdstrike-microsoft-windows-it-outage-bsod-airlines-banks-down

Checkpoint #4

State of Data Most Relevant to the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Data in Transit (Data in Motion)	Target	Attackers installed malware on point-of-sale systems to capture and exfiltrate payment card data as it was being processed and transmitted.	U.S. Senate Committee on Commerce, Science, and Transportation. (2014, March 26). *A 'Kill Chain' Analysis of the 2013 Target Data Breach*. https://www.commerce.senate.gov/2014/3/a-kill-chain-analysis-of-the-2013-target-data-breach
Data at Rest (Data in Storage)	Equifax	The breach involved hackers accessing and stealing a massive volume of sensitive personal and financial data stored in Equifax's databases.	Federal Trade Commission. (2024). *Equifax Data Breach Settlement*. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
Data in Use (in Process)	Knight Capital	The financial loss was caused by an error in an automated trading system while it was actively processing trades, demonstrating a vulnerability in data in use.	Heusser, M. (2012, August 8). *Software testing lessons learned from Knight Capital fiasco*. CIO. https://www.cio.com/article/2393228/software-testing-lessons-learned-from-knight-capital-fiasco.html
Data Life Cycle Management	AT&T	AT&T retained older customer records that were later breached, showing weak data life cycle management practices.	Caltrider, R., & MacDonald, M. (2024, July 12). *AT&T had a huge data breach: Here's what you need to know*. Mozilla Foundation. https://foundation.mozilla.org/en/privacynotinclud had-a-huge-data-breach-heres-what-you-need-to-know/
Data Integrity	NASA	The Mars Climate Orbiter was lost due to a unit conversion error, a data integrity failure where incorrect data led to mission failure.	Think Reliability. (n.d.). *Root Cause Analysis - The Loss of the Mars Climate Orbiter*. https://www.thinkreliability.com/cases/root-cause-analysis-the-loss-of-the-mars-climate-orbiter/
Data Masking/Obfuscation	Yahoo	Yahoo relied on weak hashing that failed to mask user passwords effectively, showing inadequate obfuscation.	Stempel, J., & Finkle, J. (2017, October 3). *Yahoo says all 3 billion accounts hacked in 2013 data theft*. Reuters. https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-3-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1
Data Ownership and Stewardship	Equifax	Equifax failed to demonstrate responsible stewardship of SSNs and other personal data, resulting in significant harm.	Federal Trade Commission. (2024). *Equifax Data Breach Settlement*. https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement
Data Backups and Recovery	Colonial Pipeline	The ransomware attack encrypted the company's data, making their data backup and recovery strategy central to the incident and their decision to pay the ransom.	Wood, Z. (2023, April 18). *Cybersecurity Policy Responses to the Colonial Pipeline Ransomware Attack*. Georgetown Journal of International Affairs. https://gjia.georgetown.edu/2023/04/18/cybersecu policy-responses-to-the-colonial-pipeline-ransomware-attack/

Checkpoint #5

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Broken Access Control	Yahoo	Weak account recovery questions and insufficient access control allowed attackers to access accounts.	Nelson, J. (2024, February 21). *10 Years After Yahoo Breach, What's Changed? (Not Much)*. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/10-years-after-yahoo-breach-whats-changed-not-much-
Cryptography Failure	Yahoo	The sheer scale of the breach (3 billion accounts) and the exposure of hashed passwords suggest weaknesses in their cryptographic implementation.	Stempel, J., & Finkle, J. (2017, October 3). *Yahoo says all 3 billion accounts hacked in 2013 data theft*. Reuters. https://www.reuters.com/article/us-yahoo-cyber/yahoo-says-all-3-billion-accounts-hacked-in-2013-data-theft-idUSKCN1C82O1
Injection	Ticketmaster	The provided source states that the breach involved SQL injection attacks on the company's databases.	Security Magazine. (2024, May 31). *Security Leaders Respond to Ticketmaster Breach*. https://www.securitymagazine.com/articles/10107 security-leaders-respond-to-ticketmaster-breach
Insecure Design	Target	The network design allowed third-party vendor credentials to access POS systems, a design flaw exploited by attackers.	U.S. Senate Committee on Commerce, Science, and Transportation. (2014). *A 'Kill Chain' Analysis of the 2013 Target Data Breach*. https://www.commerce.senate.gov/services/files/2 12f4-4468-a4e9-18f3a3a4e9bf
Misconfiguration of Security	AT&T	Outdated system configurations and insufficient protections exposed legacy data, a misconfiguration issue.	Hauari, A. (2024, July 12). *How to know if you were affected by the AT&T data breach and what to do next*. USA Today. https://www.usatoday.com/story/tech/2024/07/12/ data-breach-who-affected-what-to-do/74379292007/

Checkpoint #5

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Vulnerable and Outdated Software	Equifax	The breach was due to Equifax's failure to patch a known vulnerability in the Apache Struts web application framework.	O'Brien, S. (2017, September 8). *Giant Equifax data breach: 143 million people could be affected*. CNN Business. https://money.cnn.com/2017/09/07/technology/bu data-breach/index.html
Identification and Authentication Failure	Colonial Pipeline	The attackers gained initial access using a single leaked password for an inactive VPN account, a failure of authentication controls.	Kerner, S. M. (2022, June 6). *Colonial Pipeline hack explained: Everything you need to know*. TechTarget. https://www.techtarget.com/whatis/feature/Coloni Pipeline-hack-explained-Everything-you-need-to-know
Data Integrity Failure	SolarWinds	Attackers compromised the software supply chain by inserting malicious code into trusted software updates, a data and software integrity failure.	U.S. Government Accountability Office. (2021, July 28). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*. https://www.gao.gov/products/gao-21-105558

Factor Most Obvious in the Story	Company Involved	Reason(s) for Your Decision	Source Used to Make Your Decision (APA Citation)
Security Logging and Detection Failure	Yahoo	The fact that a breach went undetected for over two years indicates a failure in security logging and monitoring.	Nelson, J. (2024, February 21). *10 Years After Yahoo Breach, What's Changed? (Not Much)*. Dark Reading. https://www.darkreading.com/cyberattacks-data-breaches/10-years-after-yahoo-breach-what-s-changed-not-much-
Server-Side Request Forgery	SolarWinds	The supply chain compromise showed attackers leveraging trusted update mechanisms, resembling SSRF-like internal resource exploitation.	U.S. Government Accountability Office. (2021, July 28). *SolarWinds Cyberattack Demands Significant Federal and Private-Sector Response*. https://www.gao.gov/products/gao-21-105558