2025

Impact of Cybersecurity Breaches on Businesses: Financial Losses and Reputational Damages

BY VIGNESH MANEESH KUMAR
SUPERVISED BY DR. LORNA DODDS

Table of Contents

Aims and Objectives

1.1 Research Aim: To evaluate the impact caused to corporations due to cyber-attacks caused by threat actors with a focus on financial, reputation and data losses along with potential solutions on how to avoid and overcome these risks.

1.2 Research Objectives:

- Research Objective 1
  - Assess the Financial loss faced by companies during and after cyberattacks such as government fines for improper cybersecurity practices or ransomware attacks.
- Research Objective 2
  - Evaluate reputational loss faced by companies and its influence on business stability and stakeholders' trust based on studies and data already available.
- Research Objective 3
  - Identify effective strategies and best practices to avoid cyber-attacks and enhance cybersecurity resilience.

Analysis

1. Financial Losses Faced by Companies

Financial losses caused due to successful cyberattacks could cause serious repercussions which could take the form of government fines, direct monetary losses caused by the attack, and fluctuations in stock price. Analysing these different types of financial damage helps to understand how vulnerable companies are and how one breach can affect both their short-term operations and long-term market value.

1.1 Government Fines and Regulatory Penalties

The nature of fines and penalties imposed by government bodies on companies after the cyber-attack or breach mainly depend on the impact of the breach, as well as whether it was caused by negligence or poor cybersecurity practices.

In 2019, an unauthorised individual who was a former Amazon Web Services employee was able to gain access to personal information of Capital One's customers which roughly amounted to 100 million individuals in the United States and 6 million individuals in Canada (Capital One, 2019). The company was fined 80 million dollars by The Office of the Comptroller of the Currency (OCC, 2020). This was due to the OCC's belief that the bank failed to have proper risk assessment procedures before migrating their IT operations to the public cloud environment (OCC, 2020). The OCC also stated that the problems found were unsafe and did not comply with 12 C.F.R. Part 30, Appendix B, which is the Interagency Guidelines Establishing Information Security Standards.

Similarly, in 2022, some hackers gained unauthorised access to some of the systems of the health and care division of Advanced Computer Software Group. They did so by using a customer's account that did not have Multi-Factor Authentication. They attacked these systems which resulted in massive disruptions of services such as the NHS 111. The hackers were able to obtain personal information of 79,404 people. The Information Commissioner's Office (ICO) conducted investigations and found that Advanced did not have sufficient security measures in place. This resulted in a fine of £3 million (Landi, 2025).

In both these incidents, the companies were found to have ignored or failed to implement necessary security controls. Government agencies and other regulatory bodies clearly demand that companies, especially those handling the public's personal data, to follow proper cybersecurity measures.

1.2 Stock Price Fluctuations and Stakeholder Trust

Stock prices are crucial for corporations, and successful cyberattacks and data breaches can significantly impact it as stock prices can react sharply almost immediately. For example, in the following day after Capital One publicly acknowledged the data breach, as seen in figure 1.2, the company's share price reduced by approximately 6% which at the time equated to 2.77 billion dollars. Additionally, the company lost 100 million dollars incrementally due to this data breach (Issayeva et al., 2024). Another example is the Equifax cyber breach in 2017 which resulted in the compromise of information of 143 million customers in the United States. The hackers were also able to access credit card numbers of 209 thousand customers among other information as well (BBC, 2017). The pattern from the Capital One incident also appears here as Equifax's share price dropped by 13% in the next day and the stock fell approximately 31%, which amounted to $5 billion over the week (Melin, 2017) as seen in figure 1.1.

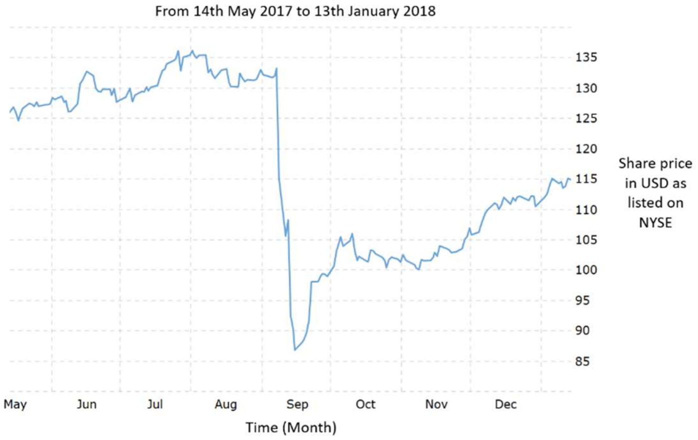


Figure 1.1 Equifax stock price (USD) showing a significant drop after the breach was disclosed in September 2017 (Macrotrends, n.d.)

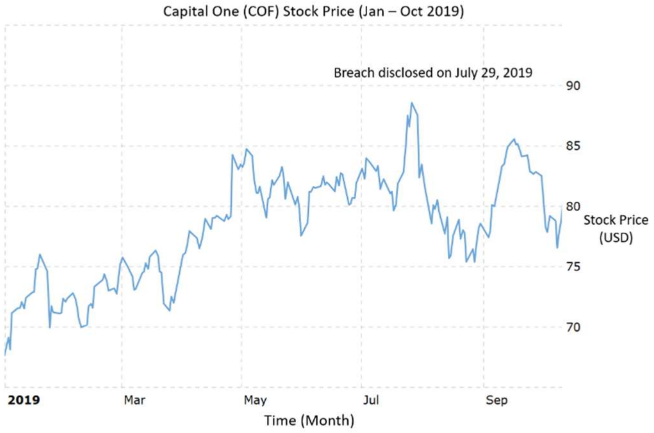


Figure 1.2 Capital One stock price (USD) showing a significant drop after the breach was disclosed in July 2019 (Macrotrends, n.d.)

While these losses are often seen as direct financial consequences of the breach, recent research shows that the stock market does not only react to the breach itself but also to the new information it reveals about the company's cybersecurity standards and procedures

(Kamiya et al., 2021). According to (Kamiya et al., 2021), shareholder wealth losses are comparatively more than the actual out-of-pocket expenses.

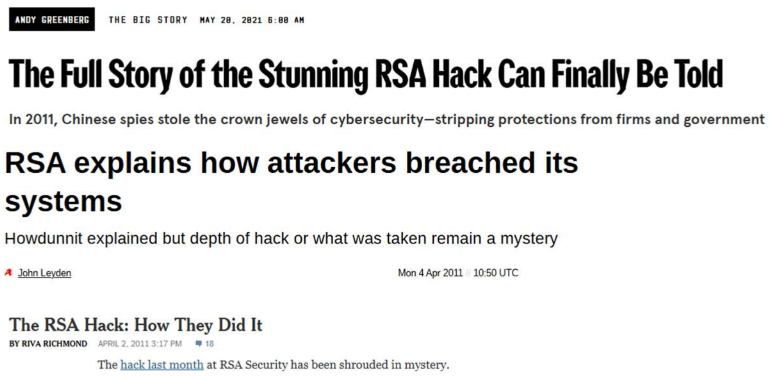
Their study shows that out of a $24.99 billion total shareholder wealth loss across multiple breaches, only $1.7 billion was due to measurable direct costs such as legal fees, government fines and compensation. The rest of the loss was due to the reputational effects such as decline in stakeholder trust, drop in sales growth, and other factors. Kamiya et al. (2021) continues to elaborate that breaches that involve personal financial information were found to cause more damage to the company's market value. In some cases, even competing companies that were not directly attacked experienced drops in share prices, as the breaches tend to create fear across the affected industry. Furthermore, it is important to understand that the drop in stock price is tightly connected to reputational damage and loss of stakeholder confidence, which will be discussed further in following section.

2. Reputational Losses and Stakeholder Trust

When a firm is affected negatively by an unexpected event like a cyberattack, its stakeholders usually become reluctant in transacting on the same favourable terms which were agreed upon before the event. This loss that occurs when these stakeholders demand better and more favourable terms due to the risk they see in transacting with the firm again is called a reputational loss (Kamiya et al., 2021).

2.1 Loss of Customer Trust and Brand Damage

In 2011, hackers were able to gain unauthorised access to restricted sections of RSA's network. They sent spear phishing emails to low level employees with a file named "2011 Recruitment Plan". Their target was the proprietary information which was linked to the SecurID token system which they required to attack other security organisations. RSA was able to detect the attack but could not prevent the confidential information from being stolen as it was too late (Watson, 2014). Similar to the incidents involving Capital One and Equifax, after RSA announced to the public that they were hit by a cyberattack, they faced a lot of public criticism, scrutiny from their stakeholders and media backlash (Greenberg, 2021) as shown in figure 2.1. All this scrutiny stem from the fact that 40 million businesses heavily relied on RSA's SecurID range of products to keep their networks safe from intruders.



ANDY GREENBERG THE BIG STORY MAY 28, 2021 6:00 AM

The Full Story of the Stunning RSA Hack Can Finally Be Told

In 2011, Chinese spies stole the crown jewels of cybersecurity—stripping protections from firms and government

RSA explains how attackers breached its systems

Howdunnit explained but depth of hack or what was taken remain a mystery

John Leyden Mon 4 Apr 2011 // 10:50 UTC

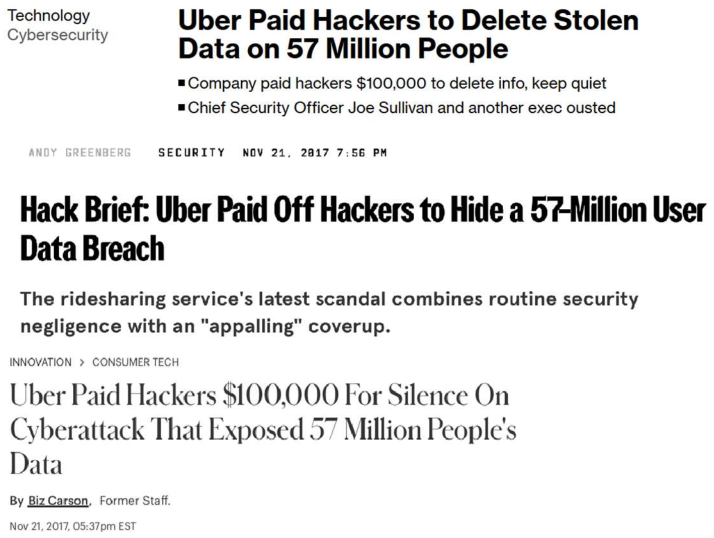
The RSA Hack: How They Did It

BY RIVA RICHMOND APRIL 2, 2011 3:17 PM 18

The hack last month at RSA Security has been shrouded in mystery.

Figure 2.1 Media covering the RSA cyberattack (Richmond, 2011; Leyden, 2011; Greenberg, 2021)

Across these events, one pattern has been identified. When a company's core service or data is compromised, especially in cybersecurity, it becomes difficult to restore customer confidence, leading to long-term reputational damage and loss of stakeholder trust.



Technology
Cybersecurity

Uber Paid Hackers to Delete Stolen Data on 57 Million People

- Company paid hackers $100,000 to delete info, keep quiet
- Chief Security Officer Joe Sullivan and another exec ousted

ANDY GREENBERG SECURITY NOV 21, 2017 7:56 PM

Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach

The ridesharing service's latest scandal combines routine security negligence with an "appalling" coverup.

INNOVATION > CONSUMER TECH

Uber Paid Hackers $100,000 For Silence On Cyberattack That Exposed 57 Million People's Data

By Biz Carson, Former Staff.

Nov 21, 2017, 05:37pm EST

Figure 2.2 Headlines about the 2017 Uber Incident (Greenberg, 2017; ;)

Media coverage related to companies affected by cyber-attacks tends to negatively impact their reputation. According to Panico et al. (2014), media coverage on the state of a company influences the general public's views and approval of the company. They emphasised that negative press can further damage a company's reputation beyond the effects of the incident itself.

In 2016, Uber was involved in a serious data breach. Hackers were able to steal personal data of 57 million users and 600,000 drivers which included names, driver's license information, email addresses and so on (Newcomer, 2017). Uber paid $100,000 as a payout to the hackers to keep the breach quiet. The following year, their CEO issued a public statement admitting to the breach (Newcomer, 2017). As seen in figure 2.2, the headlines posted by popular media outlets focused heavily on the year long cover-up, which led to greater public scrutiny and reputational harm.

Overall, reputational harm by a cyber incident could have long lasting effects. Customers, stakeholders and the public may hesitate to transact and interact with the company in the same way before the incident. As shown in examples of Equifax and RSA, reputation could impact the stock and overall value of the company which also leads to financial damages. Uber and RSA faced legal attention and public backlash from the government agencies and the public which shows how quickly trust and reputation could be damaged. Rebuilding it takes time, transparency, and best cybersecurity practices.

The cases of Equifax, Advanced Computer Software Group, RSA, Capital One, and Uber all highlight how breaches can trigger financial penalties, media scrutiny, drops in stock value, and lasting damage to reputation. These incidents show a repeating pattern of weak internal systems and poor crisis management. Research objective 3 which highlights some optimal cybersecurity practices and frameworks will be discussed further in the recommendations section due to word limit constraints and its solution-based nature.

Discussion

In this research, the case studies shows that cybersecurity incidents often lead to significant financial losses through government fines and stock market reactions by shareholders. Additionally, reputational losses often result in long term implications such as loss of stakeholder confidence and public trust which could impact the overall stability of a firm. As discussed in the analysis, Capital One and Advanced Computer Software Group were fined by government agencies due to poor cybersecurity compliance measures, while Equifax and Capital One suffered major drops in their stock price after disclosing their breaches to the public. The negative media coverage, specifically in the cases of Uber and RSA, further worsened their reputation.

Moreover, all the case studies are consistent with the findings of Issayeva et al. (2024) which argues that firms face a drop in their stock value after the public disclosure of the firm dealing with a cyber-attack. In some cases, large firms such as Capital One and Uber have the financial means to sustain themselves. However, the financial losses due to drop in stock price are often larger than the direct costs involved. Kamiya et al. (2021) considered 75 cyber-attacks among which the firms involved collectively lost $104 billion in shareholder value. Furthermore, only $1.2 billion of that was due to regulatory fines, IT and business recovery costs. This illustrates the reputational harm and loss of customer trust which could cause the shareholders to lose confidence. This results in the stock prices declining sharply. This could cause a firm to destabilise and threaten its survival.

Additionally, resources used to innovate within a firm would be reallocated towards recovering from the cyberattack. This is supported by He et al. (2020) which show that firms that have been affected by a cybersecurity breach, spend less on research and development compared to their competitors who were not targeted. In the year after the breach, they found that firms spend 10% less on research and development. This ties into the findings of Issayeva et al. (2023) and Kamiya et al. (2021). They draw attention to much of the financial loss stemming from shareholders' uncertainty due to the potential reduced competitiveness and weakened future performance following a cybersecurity incident. By cutting back on research and development, companies risk lagging behind their competitors which could lead to lower profits, slower growth and declining share value. This shows that financial consequences faced by a company affected by a cyberattack is much more than regulatory fines and direct out of pocket expenses.

However, cyber-attacks may not be the only reason for the sharp decline in share prices. Share prices could be influenced by internal and external factors. Some internal factors include profitability, liquidity, changes in strategy within the company and market value. And external factors include government regulations, variation of exchange rate between currencies, interest rates and state of inflation (Harjadi *et al.*, 2023). Furthermore, companies with high debt are more vulnerable as shareholders might view them as a risk, especially after a cybersecurity incident (Harjadi *et al.*, 2023). This suggests that the share prices could also fluctuate considering the breach and the company's overall financial health at the time.

Although the primary focus of this project is the impact of breaches on businesses, it has also drawn attention to the shortcomings of the case studies discussed above. The Capital One incident occurred due to insufficient risk assessment strategies during cloud migration (Capital One, 2019) while RSA's incident highlighted the lack of employee training on social engineering threats (Watson, 2014) and other best cybersecurity practices. Advanced Computer Software Group failed to enforce best secure authentication practices with all their customers such as lack of Multi Factor Authentication which led to the NHS being compromised (Landi, 2025). And finally, in Equifax's case, hackers exploited a vulnerability in their website application (BBC, 2017). All these observations are tied to Objective 3, which will further be discussed in the recommendations section with specific practical measures including regular staff training, routine audits, transparency and zero-trust frameworks (Chapple et al., 2021).

One of the strengths of this research is its use of real-world case studies from diverse industries, which gives it practical relevance. This approach made identifying weaknesses and patterns in how businesses are impacted by cyberattacks and breaches, possible. The diverse range of academic as well as editorial sources provided an unbiased view of the case studies. However, there are some limitations in this project that needs to be highlighted. As mentioned in the research proposal, the study relies heavily on secondary sources and public data, which could not completely capture specific details of each incident. It is difficult to measure public opinion without conducting surveys and acquiring primary data which is outside the scope of this project. This project only focused on the immediate repercussions of a cyber-attack and could not highlight how and when firms recovered if they were able to. Finally, the criteria that government agencies and regulatory bodies use to impose fines on companies could not be explored due to time, scope and word limit constraints.

Altogether, these findings align with the research objectives mentioned at the start of the study. It primarily evaluates research objective 1 and 2 by examining the financial losses and reputational effects of firms when facing a cyberattack. Furthermore, objective 3 will be further explored in the recommendations section since it is more solution focused.

Conclusion

In conclusion, this research successfully addressed its aim of analysing the impact of cybersecurity breaches and attacks that companies face, specifically, the financial and reputational losses with real world examples and academic sources. Across all the case studies, it is clear that such incidents have significant impacts on the survivability and overall share value of the firm as well as reputation. The stocks of Capital One and Equifax dropped sharply, resulting in billions of dollars wiped from their market value in the stock market. Furthermore, they were also issued regulatory fines by government agencies due to loss of personal data of their users. Uber and RSA faced huge reputation hits due to backlash from the media and the general public. This aligns with Kamiya et al. (2021), who argued that shareholder value losses are also caused by reputational losses, instead of out-of-pocket costs like legal and IT recovery expenses alone. Additionally, firm innovation is also affected by these cyber-attacks have on companies. Usually, when they are hit by cyber-attacks and breaches, they tend to reduce research and development budgets as they reallocate those funds towards business continuity and recovery, which may affect their long-term competitiveness (He et al., 2020).

Additionally, this research illustrates reputation of a company is influenced by media coverage and the opinion of the general public. In Uber's case, they handed a payout to the hackers in an attempt to cover up the breach which backfired (Carson, 2017), leading to significant reputational loss. This aligns with the findings of Panico et al. (2014) which argue that media coverage plays a powerful role in influencing a firm's reputation during and after a cybersecurity incident. For firms in sectors that deal with highly sensitive personal user data, like finance or healthcare, reputational risk is very high. The examples of Advanced Computer Software Group and RSA show how inadequate implementations of security measures such as lack of multi-factor authentication or not conducting regular staff training can have major consequences.

This study advocates that cyberattacks are not just technical issues. They are strategic business risks. The cases evaluated across this study reveal that weak internal systems, poor risk assessments, inadequate security protocol and a lack of transparency during cyber crises often increase the damage. Moreover, the harm caused due to these cyber-attacks and data breaches is not limited to the firm affected. They often affect its stakeholders and entire industries. This shows the urgent need for reinforcement of security strategies and protocols in companies, some of which will be discussed in the following section.

Recommendations

Further research could evaluate how companies that faced cyber-attacks were able to survive both financially and reputationally in the long term. This could include tracking their stock market performance or conducting long-term case studies of firms post-attack. Additionally, primary data regarding public opinions about companies and organisations involved in a cyber-attack could be collected through surveys and interviews. This could aid companies in creating a more transparent method of communication with its stakeholders.

Effective Cybersecurity Strategies and Best Practice

One of the most common vulnerabilities identified in organisations is the lack of cyber awareness among employees. Moller (2023) stresses that every organisation should prioritise cybersecurity awareness among their employees due to the increased number and variety of attacks. Some types of cyberattacks include ransomware attacks, social engineering attacks, Trojan virus attack and zero-day exploits (Moller, 2023). These attacks often rely on human error, making employees the first line of defence. It is vital to ensure that employees are regularly trained in order to avoid incidents similar to the RSA breach. Lower-level employees at RSA received a file named “2021 Recruitment Plan” and opened it without verifying its source (Watson, 2014). This resulted in the compromise of sensitive data which could have been avoided with structured cybersecurity awareness programmes.

Another good practice would be implementing the Role-Based Access Controls (RBAC) in terms of authentication, both to access physical facilities and IT. Chapple et al. (2021) illustrate RBAC as the ability of a subject to access an object based on their role or tasks that have been assigned to them. They further specify that RBAC is implemented by administrators using groups. This minimises any risk of unauthorised access, protects sensitive data and ensures that employees only access they need for their role and assigned tasks (Chapple et al., 2021).

Finally, companies should regularly conduct internal and external audits of their security controls and protocols. Chapple et al. (2021) defines auditing as the process of recording and tracking a subject, in this case, security protocols, with documentation or logs. It also involves detecting suspicious and unauthorised activities. These audits help companies identify vulnerabilities in existing controls and ensure that everything is in compliance with the regulations. Chapple et al. (2021) suggests that an independent third-party auditor are able to provide unbiased reviews and feedback on the firm’s security infrastructure. Liu and Babar (2024) argue that firms that regularly audit their security protocols were able to detect anomalies earlier and respond more effectively which prevented many attacks from escalating into dire situations.

Reference list

BBC (2017) ‘Massive Equifax data breach hits 143 million’, BBC, 8 September. Available at: https://www.bbc.co.uk/news/business-41192163 (Accessed: 12 May 2025).

Capital One (2019) Information on the Capital One Cyber Incident. Available at: https://www.capitalone.com/digital/facts2019/?msockid=0e96c8c24e0861bd2ef5ddb94f396055 (Accessed: 30 April 2025).

Carson, B. (2017) ‘Uber Paid Hackers $100,000 For Silence On Cyberattack That Exposed 57 Million People's Data’, Forbes, 21 November. Available at: https://www.forbes.com/sites/bizcarson/2017/11/21/uber-hack-payoff-57-million-data-exposed/ (Accessed: 12 May 2025).

Chapple, M., Stewart, J.M. and Gibson, D. (2021) *(ISC)² CISSP Certified Information Systems Security Professional Official Study Guide*. 9th edn. New Jersey: John Wiley & Sons, Inc.

Greenberg, A. (2017) ‘Hack Brief: Uber Paid Off Hackers to Hide a 57-Million User Data Breach’, Wired, 21 November. Available at: https://www.wired.com/story/uber-paid-off-hackers-to-hide-a-57-million-user-data-breach/ (Accessed: 12 May 2025).

Greenberg, A. (2021) The Full Story of the Stunning RSA Hack Can Finally Be Told. Available at: https://www.wired.com/story/the-full-story-of-the-stunning-rsa-hack-can-finally-be-told/ (Accessed: 2 May 2025)

Harjadi, D. et al. (2023) 'Analysis of Fundamental Factors Affecting Stock Prices', JURISMA : Jurnal Riset Bisnis & Manajemen, 13 (1), pp. 13-24. Available at: http://dx.doi.org/10.34010/jurisma.v13i1.9440.

He, C.Z., Frost, T. and Pinsker, R.E. (2020) 'The Impact of Reported Cybersecurity Breaches on Firm Innovation', Journal of Information Systems, 34 (2), pp. 187-209. Available at: http://dx.doi.org/10.2308/isys-18-053.

Issayeva, G.K. et al. (2024) 'The Impact of Cybersecurity Breaches on Firm’s Market Value: the Case of the USA', Ėkonomika (Alma Ata, Kazakhstan), 18 (4), pp. 200-219. Available at: http://dx.doi.org/10.51176/1997-9967-2023-4-200-219.

Kamiya, S. et al. (2021) 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', Journal of Financial Economics, 139 (3), pp. 719-749. Available at: http://dx.doi.org/https://doi.org/10.1016/j.jfineco.2019.05.019.

Landi, M. (2025) *Software provider fined £3m over ransomware attack that hit NHS services.* Available at: https://www.independent.co.uk/news/business/software-provider-fined-ps3m-over-ransomware-attack-that-hit-nhs-services-b2722293.html (Accessed: 2 May 2025)

Leyden, J. (2011) ‘RSA explains how attackers breached its systems’, The Register, 4 April. Available at: https://www.theregister.com/2011/04/04/rsa_hack_howdunnit/ (Accessed: 7 March 2025).

Liu, C. and Babar, M.A. (2024) 'Corporate cybersecurity risk and data breaches: A systematic review of empirical research', Australian Journal of Management. Available at: http://dx.doi.org/10.1177/03128962241293658.

Macrotrends (n.d.) Capital One Financial - 2019 *Stock Price History, COF*. Available at: https://www.macrotrends.net/stocks/charts/COF/capital-one-financial/stock-price-history (Accessed: 13 May 2025).

Macrotrends (n.d.) *Equifax - Stock Price History, EFX*. Available at: https://www.macrotrends.net/stocks/charts/EFX/equifax/stock-price-history (Accessed: 13 May 2025).

Melin, A. (2017) *Three Equifax Managers Sold Stock Before Cyber Hack Revealed.* Available at: https://www.bloomberg.com./news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

Moller, D.P.F. (2023) 'Guide to Cybersecurity in Digital Transformation: Trends, Methods, Technologies, Applications and Best Practices'. Available at: http://dx.doi.org/10.1007/978-3-031-26845-8.

Newcomer, E. (2017) ‘Uber Paid Hackers To Delete Stolen Data On 57 Million People’, Forbes, 21 November. Available at: https://www.bloomberg.com/news/articles/2017-11-21/uber-concealed-cyberattack-that-exposed-57-million-people-s-data (Accessed: 12 May 2025).

OCC. (2020) *OCC Assesses $80 Million Civil Money Penalty Against Capital* One [Press release]. 6 August. Available at: https://www.occ.gov/news-issuances/news-releases/2020/nr-occ-2020-101.html (Accessed 30 April 2024)

Panico, M., Raithel, S. and Michel, E. (2014) 'The Effect of Media Coverage on Employer Reputation', Journal of Media Economics, 27 pp. Available at: http://dx.doi.org/10.1080/08997764.2014.963228.

Richmond, Riva. (2011) ‘The RSA Hack: How They Did It’, The New York Times, 2 April. Available at: https://archive.nytimes.com/bits.blogs.nytimes.com/2011/04/02/the-rsa-hack-how-they-did-it/ (Accessed: 7 March 2025).