

Ipad's security breach

[Business](#)



Introduction Hacking into other companies websites has become a common practice with some companies.

There are various reasons for this practice which is viewed by many as unethical behavior. One of the reasons is for competitive advantage, which is gaining access to competitive strategies used by another company or destroying the corporate image of the company by exposing its weaknesses (Boone & Kurtz 2010). Hacking can also be done by security firms in order to gain access to vital data that can help in security operations. A group of hackers took advantage of the weaknesses of AT&T website and obtained e-mail addresses of people. We shall discuss the possible objectives of the Goatse Security Company in Hacking the AT&T's website together with the ethical issues arising from the practice of hacking. Goatse Security Firm's Possible Objectives When They Hacked Into AT&T's Website One of the possible objectives of the security company's action of hacking into AT&T's web site was to gain access to the users' ipad.

This would enable the Security Company to act as the users of the ipad and gain access to information being relayed by the real user. This is the reason why the targeted people were mostly top government officials. The information would probably be used for criminal activities such as fraud, gaining access to the government security details and other criminal activities. Another possible objective of the company is to shame the AT&T's company and make it feel quilt. By hacking into their website, the security company would have portrayed the AT Company as inefficient and unable to protect the identities of its clients, thus tainting its corporate image.

This would have been probably caused by competition between AT Company with another company or mere malice (Harris 2008). Case Against Computer Hacking As An Ethical Corporate Strategy For Computer Security Firms.

Some computer security companies use computer hacking as a corporate strateg in order to gain a competitive edge over their competitors. This is by gaining access to other companies' websites thus shaming the company together with the security company that developed the security system of the website. This strategy is unethical and should be discouraged (Boone \$ Kurtz 2010).

The practice of gaining competitive advantage through computer hacking compromises on privacy of a company and its clients. This is not good since privacy is a basic right to every company or individual. The practice also makes the affected company to incur costs such as law suits, compensation paid to affected clients, cost of rebuilding the corporate image and others. Computer hacking causes loss and waste of resources to the aggressor and the affected company. This practice is also illegal and is considered malicious (Salehnia 2002).

Competition should not be conducted through illegal ways and may result to criminal charges. Discuss Whether Or Not Gawker Media Acted Socially Responsible When It Reported The Security Breach Before Apple And/or AT&T Had Responded To The Public. According to me, Gawker media did not act responsibly in reporting the security breach before Apple and AT&T Companies could respond to the public. It should have allowed the affected companies to first conduct their investigations and respond to the security issue.

<https://assignbuster.com/ipads-security-breach/>

This is because it would be good for the affected people to be notified of the security breach by the affected companies and not through the media. This would have made the security breach seem less serious. Learning the breach through the media served to aggravate the magnitude of the breach and cause more worries to the affected individuals (Boone & Kurtz 2010). Gawker media also did not give AT&T and Apple companies an opportunity to defend itself in the public and to conduct the affected people personally. As The AT&T CEO, Discuss How You Would Respond Differently To This Security Breach The response by the AT&T CEO to the security breach was not adequate.

The company sends emails to all iPad users apologizing for the security breach and accused Goats media of malice in uncovering the breach. The company also suspended its services in order to put its house in order. These moves were good since they sought to regain user loyalty and give the company time to investigate the breach but they were not enough. If I were the CEO, I would send emails to all the users apologizing for the breach and making a promise that none of the same would be repeated. I would explain to the users the measure that the company has taken to ensure that such breach will not be repeated. I would make the plan detailed in order to make the users understand and convince them that their privacy will be guaranteed.

I would also invite reactions from the users on the breach and provide confidence in them that their views and proposals will be followed. I would not bother with accusing the Gawker Company publicly and I would have sought legal redress against Goats Security Company for the breach. The <https://assignbuster.com/ipads-security-breach/>

content that I would include in a public service announcement (PSA) informing the public of the breach and my plan to resolve the issue. In making the Public Service Announcement to inform the public of the security breach, I would make it clear to the public of the probable objectives of the hackers. The briefing would address the probable objectives of the hackers, the extent of damage and loss caused by the hackers, the plans to use to solve the issue and an apology to the affected people.

The briefing would also include an appeal to other companies to stop the unethical practice of hacking into other companies websites and also an appeal to the government to come up with policies and strict legislation to curb the practice (Boone & Kurtz 2010). Conclusion As shown in this case, computer hacking poses several problems to the victim company such loss of resources, loss of corporate image and the challenge of explaining to the users or clients the occurrence (Salehnia 2002). These challenges are made worse when the customers are directly affected by the act, like the case with AT&T and Apple companies. Computer hacking as a strategy causes more harm than good to the economy thus should not be used.