



Biting the hand that feeds IT

Ads by Google

[The Register](#) » [Security](#) » [Network Security](#) »

Original URL: http://www.theregister.co.uk/2005/03/22/business_school_hack/

Business school 'hack' raises ethical questions

By [Mark Rasch](#), [SecurityFocus](#)

Published Tuesday 22nd March 2005 12:57 GMT

Where do morality and ethics end, and criminality begin? What is the appropriate "punishment" for the crime of curiosity coupled with the act of snooping? These questions have been raised once again in the case of a number of applicants to the US' most prestigious business schools who went beyond the normal processes to sneak a peek at the status of their applications. The question is, how should the law and society deal with these individuals, and how do we build a society in cyberspace that is not only legally compliant but moral and ethical? Indeed, the larger question is, have we yet established a sufficiently coherent set of rules of right and wrong in cyberspace to pass moral (as apposed to legal) judgment on others?

The facts that led up to this most recent scenario are relatively simple, although all of the details have not yet been made public. A computer "hacker" - and the quotation marks are used for someone who goes by the moniker "brookbond" - apparently discovered a configuration defect in the way that a web interface was constructed at a company that had been contracted by many business schools to process applications. The company, Fairfax, Va. based ApplyYourself Inc. stored the current results of the applications of many business or management schools, including Carnegie Mellon, Harvard, Dartmouth, Duke Universities and Massachusetts Institute of Technology.

"Brookbond", who described himself as a specialist in information technology and software security, posted the configuration vulnerability and a script which, if inserted into a browser, would permit an individual to look at the status of his or her own application. While Brookbond has been described as a "hacker", he may or may not have (OK, he probably did) make an unauthorized access to the ApplyYourself website. At 12:15 on the morning of 2 March, 2005 Brookbond posted this information into Business Week's online technology forum, where apparently about 150 applicants read the posting and attempted (mostly without success) to see the status of their applications. The technique was also apparently reposted by a blogger named PowerYogi who added the comment: "Is it right or wrong to check status this way? Basically, we are talking about some sloppily protected software here. If you don't want someone to see it, hide it well. Welcome to the internet."

Different business and management schools took a differing approach to dealing with the curious applicants. The Harvard business school (which had the vast majority of the cases - call it Crimson ingenuity?) decided to immediately deny admission to all of the 119 applicants who attempted to go to the ApplyYourself website. In a letter to applicants, HBS Director of Admissions noted that: "Such behavior is unethical and inconsistent with the behavior we expect from high-potential leaders we seek to admit to our program." Harvard left the door open for these individuals to reapply. Stanford is reviewing each application on a case-by-case basis.

The questions raised are: "Is the conduct by the applicants morally repugnant? Should they be punished? And what should the punishment, if any, be?"

Laws and ethics

The federal computer crime law, 18 U.S.C. 1030, makes it a crime to make or attempt an "unauthorized access" into a computer used in interstate commerce with the intent to get "any information" from that computer. So the first question is whether the applicants made or attempted an "unauthorized access" into the ApplyYourself computer.

It is clear that, by using the script posted by Brookbond, applicants were able to display portions of the ApplyYourself network that were not otherwise viewable. Once typing in the modified URL, the information became publicly viewable - if not publicly accessible. However, the fact that the information became publicly viewable does not make the information public, nor does it make the access by the applicants "authorized." One of the big problems in cyberspace is the lack of workable analogies. In the "real" world, we generally know what is authorized and what is trespass without any signs, postings, or demarcations - we just kinda know.

For example, we intuitively "know" that in a hotel, there is a difference between being in the lobby (generally OK, but they can kick you out), a conference room (OK if you are attending the conference, or if the conference is *intended* to be public), a hotel room (OK if you are an employee, guest, or invitee of a guest) or the business offices (OK for employee or what the law calls "business invitee"). We also consider factors like the level of security (door or no door, lock or no lock, posting or no posting) in determining whether it is reasonable to assume that the access is authorized or not. We finally consider certain exigent circumstances in deciding whether, as a society, we are willing to accept the conduct (OK to break into a locked car to get a baby out, OK to open door of unlocked car to turn lights off).

The problem is, cyberspace is the almost complete lack of such a consensus. While the website developer may know what he or she wants to be available to the public, this may not always be the same as what had been made available to the public. Even an innocent surfer may not always know whether information floating around is intended to be public, or just happened to become so. The ordinary rules of behavior tend not to apply in cyberspace. For some reason, because we are merely sitting at a computer screen in our own den just typing, we aren't doing anything "wrong" or criminal. There is a huge tendency to blame the victim - if they didn't WANT me to break in, why didn't they have better security? And, like steroids in baseball, there is a tendency to say, "everybody is doing it" so it must be OK. For example, an individual claiming to be one of the HBS rejected applicants posted to Slashdot, stating, "Personally, I'm glad I checked my own status. Do I think I'm unethical? I'm willing to bet 90+ per cent of the people who actually saw the technique and applied to HBS in Round 2 (the round currently awaiting decisions) tried it." The applicant - showing typical entrepreneurial spirit is now selling T-shirts demanding that the "HBS 119" be freed - pronouncing "[ethical schmethical!](#)" (<http://www.cafepress.com/FreeTheHBS119>)"

It seems pretty clear that the applicants knew - or reasonably should have known - that they weren't supposed to see the status of their applications, and that the portion of the ApplyYourself website they went to wasn't supposed to be accessed by the public. In that regard, not only did they open themselves up to ethical retribution, but to potential criminal prosecution under both federal and local law. But that doesn't answer the entire question. Indeed, in the 1973 movie *The Paper Chase*, the protagonist Harvard Law student breaks into the law library with a friend to satisfy his curiosity about a contracts professor's unpublished writings. The scenario is not presented as illegal (trespass) or particularly unethical - indeed, it is almost heroic.

This is what makes the reaction of the business school admissions directors particularly subject to scrutiny. The applicants' conduct is certainly more than mere curiosity, and something less than smashing down the door of the admissions office and cracking open a file cabinet to learn the status of the application. It is also wrongful, unethical, and potentially criminal. But should HBS treat the applicants as modern Hester Prynne's, painting a Crimson "H" (for hacker) on their chests? If these individuals are truly not ethical enough to go to HBS, should they be permitted to enter the business world at all? Is this inherently unethical behavior, or a foolish mistake? After all, there is more than one moral ambiguity here.

What is the responsibility of ApplyYourself to secure the sensitive personal information they store on their site, and to test the configuration for some relatively simple scripting errors? A perusal of the "press" section of their website says nothing about the recent brouhaha - do they have any duty to warn their customers or the applicants? Did HBS or other business schools disclose to the applicants the fact that their data would be shared with or processed by third parties who may or may not have had security? What about the applicants who saw the Business

Week postings and failed to notify ApplyYourself or their respective schools - do they have moral blamefulness? And don't forget Brookbond and PowerYogi!

An ethical solution

The approach taken by Stanford is, in my opinion, more reasoned and ultimately morally more defensible than that taken by Harvard. It is OK to treat this incident as a black mark against the applicants - and a major one at that. But an unethical act does not necessarily make an unethical person. It is easy to publicly proclaim your ethical standards on the backs of others - would Harvard dismiss tenured faculty for a similar breach? Or better yet, disclaim a large grant from a donor who had done the same thing? Probably not. But most ethical breaches in business are likely crimes of opportunity. First you convince yourself that you did nothing wrong, or that what you did was morally justified. So many of these individuals should be admitted into HBS, or other prestigious business schools - not because they are morally pure, but because they are not. This should be an opportunity for HBS and the others to teach the incoming students not only how to be better managers - but more ethical ones.

Harvard University's MBA program, for example offers two courses (both of which are electives) entitled "Moral Leadership," one of which "relies heavily on classic and contemporary works of fiction... to examine in depth the practical moral issues that managers face, as individuals and as leaders of organizations." CMU's Tepper School has a mandatory course in Business Law and Ethics which, according to the course catalogue, focuses on "problems dealing with legal and regulatory matters." Stanford's MBA program includes a course in business ethics, which is designed to teach students to "consider an important set of ethics systems, increase the precision with which students think about, discuss, and practice ethics, and provide opportunities to apply ethics systems to business problems." Such ethics courses should be mandatory in all business schools, and, while we are at it, computer science and IT schools - they are already mandatory in law school.

If you have ever gotten a speeding ticket, you likely remember *exactly* where the ticket was issued, and instinctively slow down at that location. If otherwise ethical applicants who visited the ApplyYourself website are admitted, they may become the proselytizers for ethical computing - having faced significant consequences for their lapse. In the 1973 baseball movie "Bang the Drum Slowly" the players con the unsuspecting by playing a card game called "TEGWAR" - The Exciting Game Without Any Rules. That unfortunately is the state of the Internet and cyber-ethics today. Business and computing schools need themselves to step up to the plate and do more than grandstand about ethics - they need to teach it as well.

Copyright © 2004,  SecurityFocus (<http://www.securityfocus.com/>)

SecurityFocus columnist Mark D. Rasch, J.D., is a former head of the Justice Department's computer crime unit, and now serves as Senior Vice President and Chief Security Counsel at Solutionary Inc.

Related stories

[Reed subsidiary hack exposes 32,000](http://www.theregister.co.uk/2005/03/09/hackers_attack_reed/)

(http://www.theregister.co.uk/2005/03/09/hackers_attack_reed/)

[T-Mobile hacker pleads guilty](http://www.theregister.co.uk/2005/02/17/t-mobile_hacker_pleads_guilty/)

(http://www.theregister.co.uk/2005/02/17/t-mobile_hacker_pleads_guilty/)

[Open Source security manual and training for ethical hacking](#)

(http://www.theregister.co.uk/2003/02/20/open_source_security_manual/)

© Copyright 2006