Science & Technology

Why Some Companies Don't Invest in Cybersecurity

Fall 2015



J. D. King / theispot.com

In the last two years, tens of millions of Americans have had their credit-card or Social Security numbers stolen in hacking attacks against Target, Home Depot, Sony, JPMorgan Chase, and other corporations. These data breaches represent a growing problem, with losses from online credit card and identify theft in the US totaling nearly $1.7 billion in 2014.

So why don't corporations shore up their networks and better protect sensitive information? The answer, according to Benjamin Dean '14SIPA, a fellow for Internet governance and cybersecurity at the School of International and Public Affairs, is that they have little financial incentive to do so. He came to this startling conclusion by analyzing the financial reports of several corporations that experienced large-scale data breaches in recent years. He says the cost to Target of its hacking in November 2013, in which cybercriminals took forty million credit card numbers, is characteristic: the company spent $252 million afterward investigating the breach, repairing its network, and settling customers' lawsuits, but recovered most of its losses in insurance reimbursements and tax reductions that are available to companies victimized by fraud. Ultimately, Target absorbed just $105 million in damage. That may sound like a lot of money, but it represents less than 0.1 percent of the company's annual revenue.

"The costs of cybercrimes are distributed widely across society —among insurers, taxpayers, banks, and, of course, customers inconvenienced by having to straighten out their credit afterward," says Dean, who reported his findings in the online magazine *The Conversation*. "For that reason, the financial incentives for companies to invest in greater information security are low, and government intervention might be needed."

There are many things that US corporations could do to bolster their computer networks, according to Dean. He says that few corporations design their networks with adequate internal security barriers, which restrict intruders' access to small sections of a network once they are inside. Companies also do not consistently encrypt sensitive information. Sony's hackers made off with forty-seven thousand employee Social Security numbers last fall, Dean notes, by reading plain-text spreadsheets that contained this and other personal information.

"Building barriers and encrypting data can make a network more cumbersome for employees to use, so it adds to operating costs," says Dean. "It's evident that some companies are choosing not to implement certain basic protections because they

don’t seem like necessary investments.”

The US Congress is currently considering several policy proposals aimed at improving information security. Dean is among a number of critics who have complained that the bills contain few provisions that would encourage companies to make the sorts of simple security improvements that he says are needed. According to Dean, the most prominent of these bills, the Cybersecurity Information Sharing Act of 2015 (CISA), could actually make the situation worse. The legislation, currently in the Senate, would push private companies to provide information about their Internet traffic to US government agencies. The idea is that intelligence officials would study the vulnerabilities of America’s private networks and ultimately help companies improve them. But the bill, in its current form, would grant participating companies immunity from future lawsuits related to data breaches — thereby, Dean says, removing one of the few financial incentives the companies now have to improve their networks.

Beyond that, Dean says the language of the bill is so vague that it could give the government an opening to misuse its network access.

“The legislation raises serious questions about the US government’s objectives in studying Internet traffic,” he says. “For instance, will intelligence agencies be using the information they gather to develop offensive capabilities, in addition to bolstering defenses? If so, how much of their research will be devoted to either objective? A good law would spell out very clearly how individuals and companies will benefit. The CISA, in its current form, does not do that.”


Guide to school abbreviations

All categories >