

Information Security Breaches

2000 to 2007

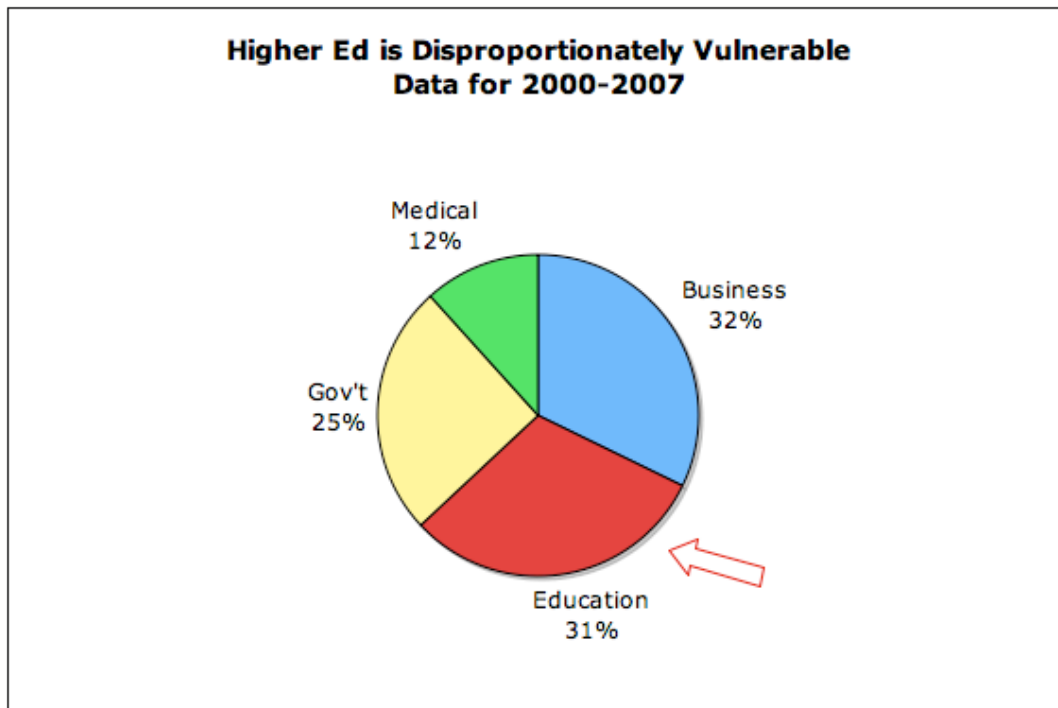
This brief analysis is based on a database of 798 publicly reported information security breaches in the US from 2000 through 2007. The raw data come from the Privacy Rights Clearinghouse (<http://www.privacyrights.org/ar/ChronDataBreaches.htm>). This analysis follows on the paper Dennis Reedy and I wrote: “Why Banks View Campuses as Risky Customers” published in the Association of Financial Professionals *Exchange* in March, 2007. You may download a copy at <http://www.walterconway.com/index.html>.

That original paper was based on data for the period 2000 to 2006, but it focused on the experience in 2006. The analysis below looks at the entire 8-year period 2000-2007 to arrive at some conclusions regarding security breaches, their causes, and their costs.

What follows is a brief statement together with an explanation and a graph of the data supporting it. Anyone interested in examining the database may download a copy of the Excel file from my website (<http://www.walterconway.com/id20.html>).

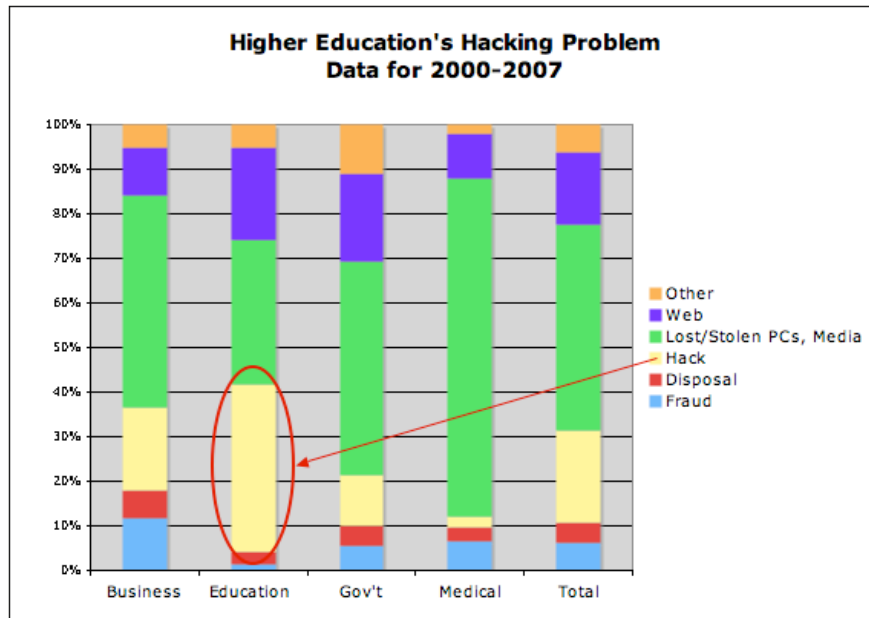
Education remains disproportionately vulnerable to a breach.

Education institutions represent a relatively small part of the payment system and the total population. Where there are a few thousand Higher Education institutions, D&B lists over 14 million businesses. It is therefore disturbing to find that Education and Business represent roughly the same percent of breaches.



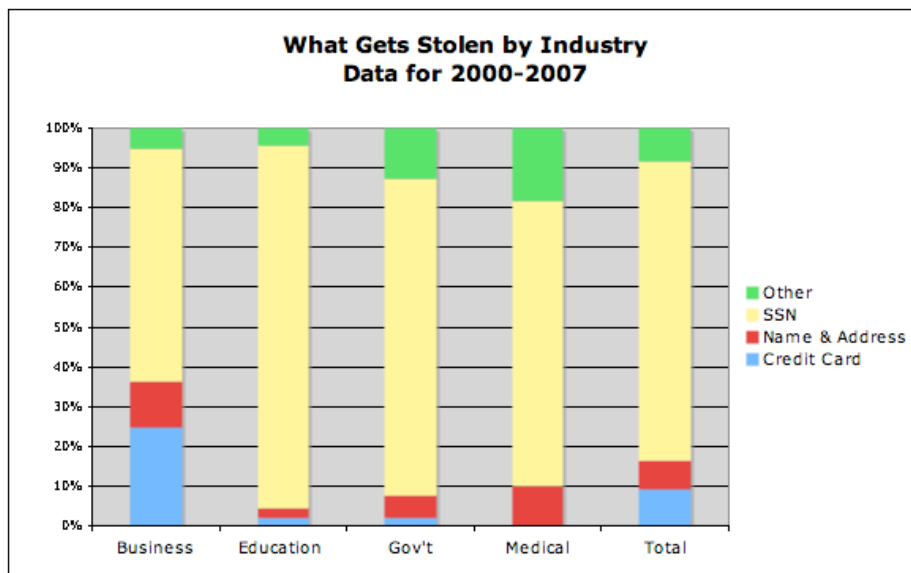
Education has a hacking problem.

Education has the largest share of hacking of any industry group. Indeed, hacking is the largest single cause of Education breaches; for all other segments lost/stolen laptops and storage devices is the biggest source of breaches. The size of the Web as a source of data compromises is disturbing. Current experience and research indicates that this is an increasingly popular threat vector. I expect this source to grow in the future.

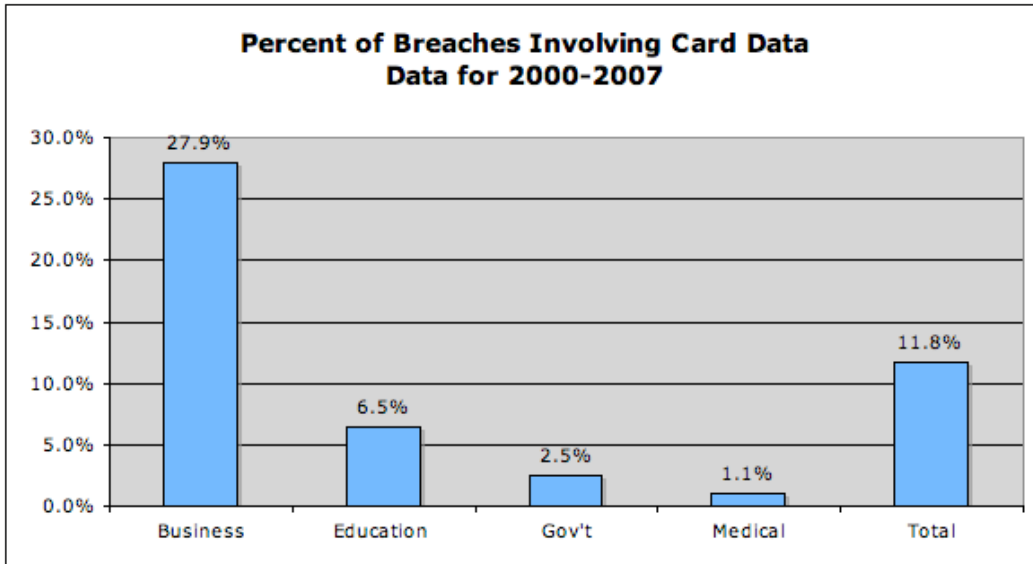


Breaches expose sensitive information, including credit card data.

The most frequently exposed data are SSNs across all industries. It is not surprising to note that Business breaches are the most likely to expose credit card data.

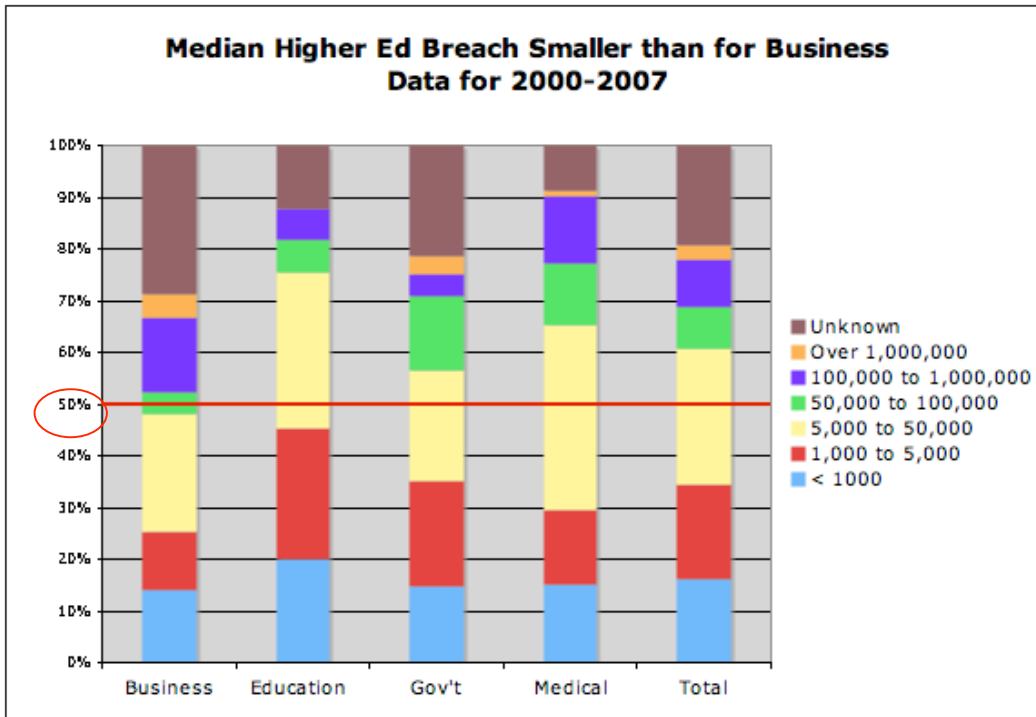


Nearly 28% of Business breaches expose credit card data, as opposed to roughly 7% for Education. It will be informative to monitor these percentages in the coming years.



The median breach for Education is smaller than for Businesses

To put a figure on the expected cost of a breach, we can use an industry average of \$197 (based on the Ponemon Institute’s 2007 survey) in direct costs. Other sources indicate a cost between \$90 and \$305. Brand damage to the institution’s reputation is not included.



Breaches are primarily externally caused.

This conclusion is the opposite of what some security experts have maintained. The data are taken from published reports and while there may be some reporting bias, the data are consistent across industry. My guess is that one could include lost laptops and storage devices in the “Internal – Accidental” category although that is not the way the data are summarized in this survey.

