Another viewpoint of interest is in quantifying the risk by threat actor – outsider, insider or partner. Outsiders were responsible for 48% of the breach incidents, and 50% of the records disclosed, making this the leading threat actor. Insiders, by comparison, were responsible for only 29% of both incidents and records disclosed. It should be noted that when a breach incident involves an Insider, it is more than twice as likely to be an accident than a malicious act.

Another interesting finding relates to when an organization engages a third party partner. The median of the records disclosed when a partner is involved is almost twice that of the records disclosed when an outsider is involved. This observation illustrates the increased risk an organization assumes when outsourcing the processing (and thus security) of their data to a third party. If this additional risk is not taken into consideration when making the decision of whether to engage the partner, the organization is operating under an inaccurate risk picture.

To get a sense of who is losing all this data, the information was broken into sectors: business, education, government, medical. Although the sectors were fairly close at the start of the study in 2005, by 2009 the business sector was the leading group of victims, responsible for more than twice the number of records disclosed than the other three combined, for a total of over 507 million records. The business sector was responsible for 49% of all incidents, compared with 20% for education, 19% for government, and 12% for medical. Within the business sector, there are some large industry categories. The largest was the financial category, responsible for over 254 million records by itself.

The breach vectors were inspected to determine if there is a type of data that is most commonly exposed in a specific attack. The highest numbers of customer and student records are divulged during hacking events, while the most of the records compromised in employee and patient data were from stolen laptops.

Finally, a cost estimate was calculated based on the Ponemon Cost of a Data Breach studies (2005 - 2008). The cost per record for each year was applied to the number of known records disclosed and the total came to over $139 billion. The problem of companies under-reporting the number of records disclosed makes this a low estimate. Over the five years of the study, the average figure of incidents reporting the number of records disclosed as “unknown” (which are counted as a zero in the database) was 34%.
Although the report published on the study has significantly more detail, this series has presented some of the highlights. One of the main challenges in researching these events is the victim organization’s unwillingness to discuss the event. Many of the events came to light only after Freedom of Information Act requests on the part of organizations like the Open Security Foundation. Until there is a Federal mandatory reporting law that also has a component of a central reporting agency, there will remain stumbling blocks to gaining access to the data.

***

Suzanne Widup, MSIA has significant experience in workplace investigation, digital forensics, e-discovery and litigation support. Her background includes 16 years of security and Unix system administration, technical support, and software development. In addition, in what doesn’t sound like much spare time, Suzanne is a certified Graduate Gemologist and a Graduate Jeweler, a certified Precious Metal Clay instructor, and the founder of the Yahoo Silk Painting group.

M. E. Kabay, PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He is Chief Technical Officer of Adaptive Cyber Security Instruments, Inc. and Associate Professor of Information Assurance in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.

Copyright © 2011 Suzanne Widup & M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.