Hal Berghel

IDENTITY THEFT AND FINANCIAL FRAUD

2010 IN REVIEW

I wear a number of hats, one of which is co-director of the Identity Theft and Financial Fraud Research and Operations Center (www.itffroc.org). Now entering its 8th year, ITFF/ROC is currently funded by the Department of Justice and, among other things, develops secure credentialing systems for crisis management and first responder applications. An important part of ITFF/ROC is community outreach, such as the ITFF/ROC Reading Room summaries of media reports of identity theft and financial fraud activity (www.itffroc.org/rr). In this column, I'll share what we've learned about these e_crime reports in 2010. 2010 was a blockbuster year for identity theft and financial fraud.

ITFF/ROC is a meta-level reporting source, we report on the major media reports of data breaches that are either directly or indirectly associated with identity theft and financial fraud crimes. We do not conduct investigations, so the data we'll summarize is third-party and drawn from major media sources. We make no claim that our summary is exhaustive. However, we would expect that our data sources are relatively independent and unbiased – or at least that any biases would be minimum, random, and offsetting. What we're primarily interested in here is the distribution of the breaches by source and type, not the total number of breaches.

Without question 2010 was one for the record book: over 3 million individual, private, and confidential record leaks were reported in the media. In fact, from January 1, 2010 to March 31, 2011, we were able to document media reports of data security breaches involving 4,206,774 individual records (see, Figure 1, below). And there is no question that this is but a small fraction of the total because most data breaches for which disclosure is not required by regulatory authorities go unreported.

So it would appear that estimates of personal record compromises affecting tens of millions of individuals are likely to be reliable; hundreds of millions would not be surprising. This number is not easily extrapolated into expected dollar amounts because there is no one-to-one correspondence between a compromised record and a specific loss for a variety of obvious reasons.

One of the more alarming facts to emerge from Figure 1 is the percentage of contribution by healthcare providers, educational

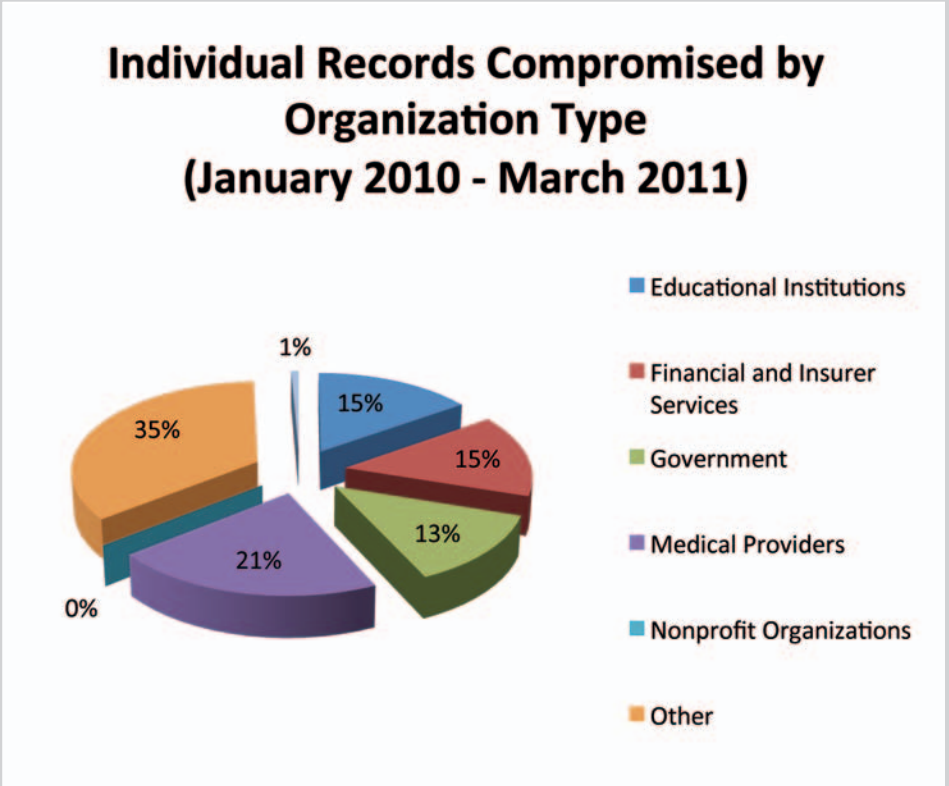

Figure 1: Distribution of the Number of Security Breach Incidents by Organization Type (source: itffroc.org)

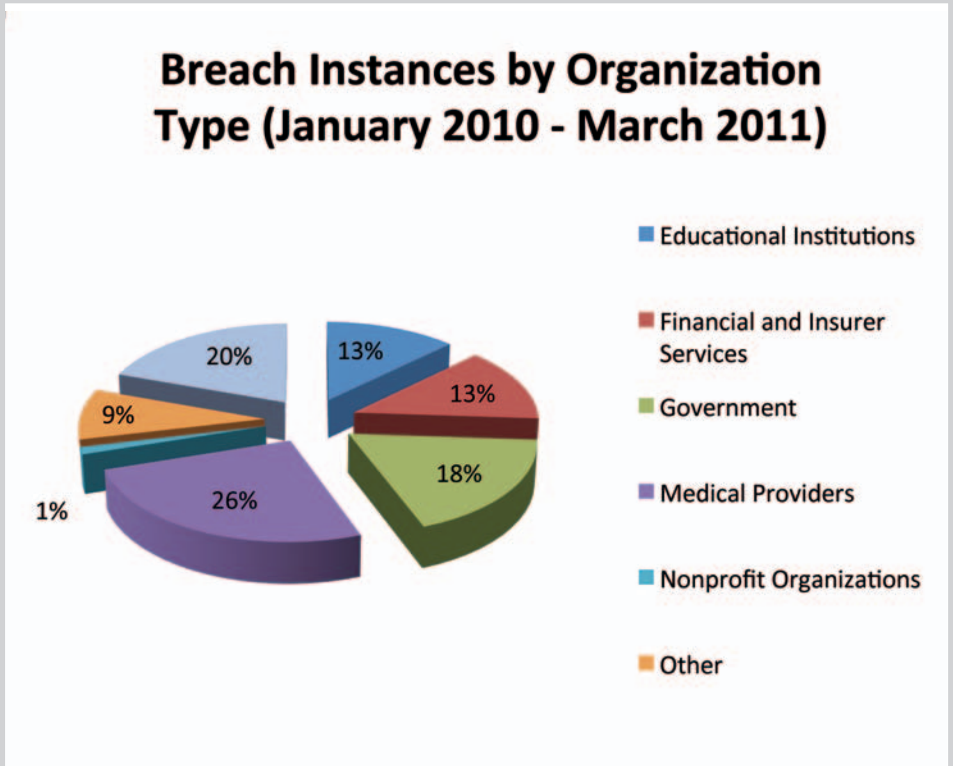
Breach Instances by Organization Type (January 2010 - March 2011)
20%
13%
13%
9%
18%
1%
26%
🟦 Educational Institutions
🟥 Financial and Insurer Services
🟩 Government
🟪 Medical Providers
🟦 Nonprofit Organizations
🟧 Other

Figure 2: The Volume of Personal Records Compromised by Type of Crime (source: itffroc.org)

institutions, and governments. These three sources collectively account for one half of the total compromises. If we can't trust our colleges, hospitals, and government agencies to protect our confidential information, who can we trust? Note that a breakout by breach instances follows the same pattern (Figure 2) with the exception that there appear to be fewer breaches in the retail arena, but the breaches tend to involve a larger than normal number of personal records. This accords with our intuition because of the number of financial card transactions processed by merchants.

However, when we shift the focus away from the organization type and toward the nature of the breach, a different picture emerges (Figure 3). Note that the majority of individual records compromised resulted from some form of online hacking.

Conclusion

Remember that ITFF/ROC aggregates media reports, it doesn't engage in investigative reporting. So we can only paint pictures with fairly broad brushes. That said, our summary seems to suggest some plausible, testable hypotheses:

The Health Insurance Portability and Accountability Act (HIPAA) does not seem to be working as well as expected when it comes to tightening up digital security. Healthcare breaches were the largest single identifiable source of individual record breaches and reported incidents. HIPAA was put into law in 1996 and the compliance deadline for the Privacy Rule was April 14, 2003! So implementation should have been completed by all covered entities by 2010.

Legislation regarding financial industry and the private sector don't seem to be doing much better. Falling right behind healthcare were financial institutions and retail. Gramm-Leach-Bliley (1999) and Sarbanes-Oxley (2002) yield disappointing results when it comes to protecting personal information.

Both of our sacred cows, higher education and governments, have been gored. Something in the way the public sector protects information is seriously deficient. If you've been following these columns you already know that the prime culprit in my opinion is a cadre of ill-prepared and uninformed executives and senior managers.

So where did we go wrong? I'll speculate on what seem to me to be several likely

Without question 2010 was one for the record book: over 3 million individual, private, and confidential record leaks were reported in the media. In fact, from January 1, 2010 to March 31, 2011, we were able to document media reports of data security breaches involving 4,206,774 individual records.

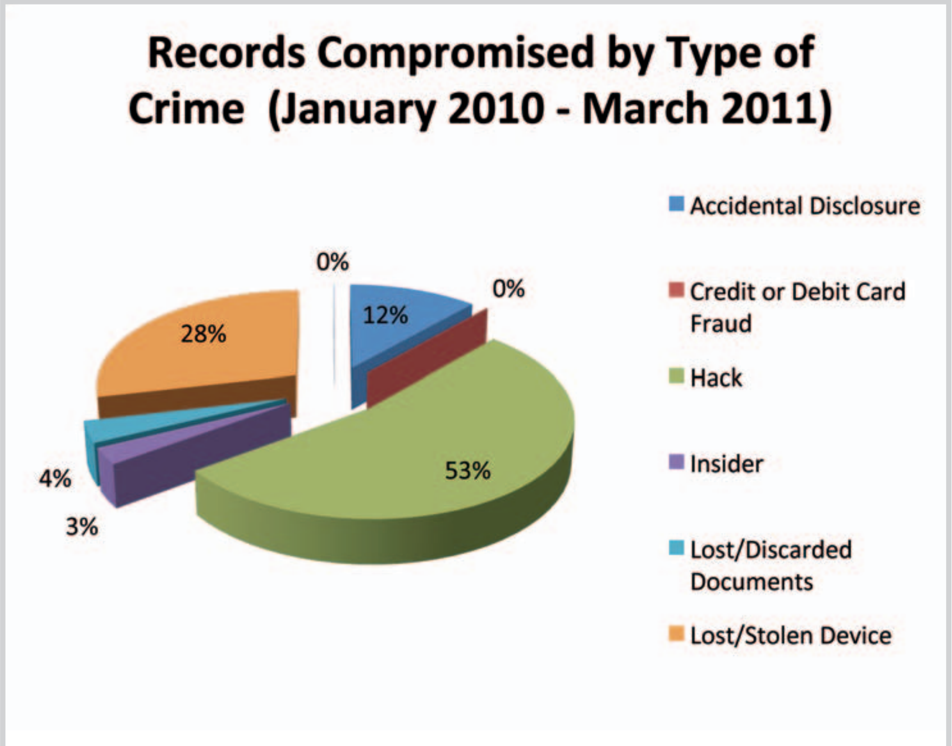

Figure 3: The Volume of Personal Records Compromised by Type of Crime (source: HYPERLINK "http://itffroc.org/"itffroc.org)

causes. First, we have spent so much attention on incident handling, that we've neglected the cornerstone of prevention: a correctly implemented and continuously monitored information security policy. The core ingredients are open and subject to change, but one thing that is never included in INFOSECPOL is the co-mingling of customer records with Internet-accessible files: read that, if you can get to it through the cloud, it probably is vulnerable!

Another obvious candidate is the use of Social Security Numbers as primary keys. That practice should never have been implemented outside of the Social Security Administration and IRS in the first place, but there certainly hasn't been any excuse for using it since the 1950s when data processing became an industry.

A third concern is the unwarranted reliance on vendor security. Does the name Heartland Payment Systems come to mind? According to the Washington Post, Heartland allowed 100 million credit and debit card accounts to be compromised in one 2009 incident! And this isn't a singular case. In June, 2005 CardSystems Solutions allowed 40 million of the same type of financial records to be compromised. Card Systems, Pay By Touch, TJX, Heartland Payment Systems… the list goes on.

There's an old adage: fool me once, shame on you; fool me twice, shame on me. Look around the next G&L Roundtable and ask who's doing thorough background checks on financial transactions processing vendors. There's part of the problem. Reliance on the vendor to provide customer transaction security is enabling behavior.

I'm entirely confident in making this prediction: when it comes to identity theft and financial fraud, we ain't seen nothing yet.

Next time I'll discuss an effective (but business-unfriendly) way to protect your privacy.

Hal Berghel is Director of both the UNLV School of Informatics and the Identity Theft and Financial Fraud Research and Operations Center (itffroc.org). His consultancy, Berghel.Net, provides security and management services to government and industry.

*I'm entirely confident in making this prediction:
when it comes to identity theft and financial fraud,
we ain't seen nothing yet.*