As organized crime goes virtual, the law cyber-saddles up

- Experian® Data Breach Resolution
- USA
- July 26 2011

Our guest blogger this week is Tom Bowers, Managing Director, Security Constructs LLC – a security architecture, data leakage prevention and global enterprise information consulting firm.

Back in the days of Prohibition, organized crime burst into the national consciousness with the “ka-pow” of a Tommy gun, capturing a sometimes romantic fascination that continues to this day. The public face of organized crime may have morphed somewhat over the years, from Al Capone and Bugsy Siegal to Vito Corleone and Tony Soprano, but the mugshots have been generally similar and the contours of “the life” familiar.

With the advent of technology, however, organized crime has flocked to new outlaw opportunities that depart wildly from the old stomping grounds. Today, cyber crime is the hot modern racket, with offenses ranging from the seemingly mundane (non-delivery of payment or merchandise top the list at 14.4% of all online crime), to the daring (scams impersonating the FBI, which come in second place at 13.2%), to the now well-known standbys (identity theft, rounding out third place at 9.8%). At the center of the cyber crime explosion is organized crime, often formed into global gangs (frequently based in Eastern Europe), ever more sophisticated, and comprising a new kind of operation that doesn’t look anything like the movies.

Indeed, cyber criminals have been so successful in recent years that they have seemed unstoppable, leaving federal law enforcement struggling with the fast pace of attacks and ever-changing tactics. The FBI gained headway – and large-scale arrests in the U.S. – with the hiring of more agents with computer science, business and operational analysis backgrounds, but cyber criminals responded by outsourcing their operations to countries with weak computer crime laws and law enforcement capabilities. Investigations across borders were bogged down
by legal proceedings, arrests and convictions were slow to materialize, and negative public outcry placed pressure on governments around the world.

But now the tide has changed. The three-year-old International Multilateral Partnership Against Cyber Threats (IMPACT) is the world’s first not-for-profit comprehensive global public-private partnership against cyber threats, bringing together academia, industry experts and governments from more than 120 partner countries. The Budapest Convention on Cybercrime, an effort to synchronize national cyber security laws, has been joined by more than 30 different countries. The European Union, U.S and NATO are working together to tackle cyber crime and have announced the formation of a new cybercrime center, to be operational by 2013.

As international agreements begin to take shape, global law enforcement benefits from common frameworks for cooperation. Accordingly, countries are beginning to share enforcement officers, time and talent…and cyber crime arrests are on the rise. Clearly, a mobilized, globalized and flexible law enforcement response to cyber criminal activity – combined with best practices for data breach prevention – are the best ways to keep today’s mob offline and on the run.