This is the second in a set of four articles by Kathleen E. Hayman, Michael Miora, CISSP-ISSMP, FBCI and Allen P. Forbes that examines the threat of cyber crime in business-to-business (B2B) activities. This part presents some top-level findings and analyses about the environment or climate affecting the activities of pirates and privateers in North America, Europe and the former Soviet Union.

* * *

Where Are the Havens?

Misha Glenny states in *McMafia: A Journey Through the Global Criminal Underworld* <http://www.amazon.com/McMafia-Journey-Through-Criminal-Underworld/dp/B002RAR108> that three factors are essential to fostering growth of cyber crime in a country. These are, “…steep levels of poverty and unemployment; a high standard of basic education for a majority of the population; and a strong presence of more traditional organized crime forms.” (p 273)

Glenny continues, “Nobody fits the bill better than the so-called BRIC nations—Brazil, Russia, India, and China. These are the leading countries among the emerging markets, the second tier of global power after the G8 (though politically Russia straddles the two).” All of these nations are attractive to corporations attempting to diversify their markets to continue or enhance their corporate competitiveness in the global market.

North America

Much of the cyber crime in North America appears to originate from within North America itself. According to the 2008 IC3 Annual Report,<http://www.nw3c.org/downloads/2008_IC3_Annual%20Report_3_27_09_small.pdf> released in March 2009 by the Internet Fraud Complaint Center (IFCC), now called the Internet Crime Complaint Center (IC3),<http://www.ic3.gov/default.aspx> Internet fraud in the US has been increasing as the global economy worsens. Most attacks on US entities are based out of the US itself, Canada, the United Kingdom, Nigeria and China.<http://www.canada.com/news/Recession+leads+surge+online+crime+report/1445039/story.html> In 2008, the most common complaints the organization received were the non-delivery of promised merchandise, auction fraud, credit card fraud, and investment scams. Perhaps non-delivery, auction fraud, and investment scams require a slightly higher degree of cultural savvy than other cyber crimes, though there is insufficient evidence to draw solid conclusions.

The IC3 report over half of known Internet fraud perpetrators resided in California, Florida, New York, Texas, District of Columbia, or Washington. These are, however, the most populous areas of the US. On a per capita basis, the District of Columbia, Nevada, Washington, Montana, Florida, and Delaware have the most perpetrators of Internet fraud.

However, organized cyber-gangs based in Eastern Europe have also been increasingly targeting
small to mid-sized US companies’ financial holdings, according to an alert released by the Financial Services and Information Sharing and Analysis Center (FS-ISAC). Since these attacks are on smaller, lesser-known companies, they do not receive the degree of media attention as the larger-scale attacks have seen. Many of these “cyber-gangs” use scamming, phishing and the more precise “spear-phishing,” a highly targeted phishing attack, in their methods.

Within the North American context, US and Canadian cyber law enforcement resources are gaining ground. Despite the controversy surrounding the creation and appointment of a US cyber security czar, the fact that such experimentation with cyber security strategies is even occurring is heartening. North America generally appears to have law enforcement entities generally sympathetic to the cyber security needs of the private sector.

**United Kingdom/Western Europe**

The United Kingdom is making great efforts to focus law enforcement resources on cyber crime. In the summer of 2009, the UK’s Association of Chief Police Officers (ACPO) published a strategy for combating cyber crime, recommending centralization of cyber crime reporting to streamline law enforcement efforts.

Additionally, the European Union has expressed interest in strengthening its cyber law penalties and improving its enforcement capabilities. Among these measures is the lengthening of prison sentences for cyber criminals to five years. The European Commission also intends to review current cybercrime legislation and revise it as appropriate; it also intends to create an EU-wide notification system for cyber attacks and to collect attack data for future analysis.

Law enforcement still has far to go to catch up with the cyber security threat. However, these nations’ serious planning and dialogue concerning cyber crime suggests sympathy with the cyber security concerns of private business.

**Russia/Eastern Europe**

Russia has a lengthy history of organized crime, the precursor to organized cybercrime. Its criminal organizations were born in the gulags during the 1920sand increased in stature and organizational capability over time. Members were required to leave their families and to rely on the organization for protection and support.

Russian cybercrime began primarily as software piracy. However, a 1994 hack of Citibank that was traced to St. Petersburg prompted a stark increase in Russia-based cybercrime. The hack allowed over $10 million to be stolen via the telephone system, with most of the money never being recovered.

During the course of the 1990s, Russian crackers were key players in developing botnets and Internet worms, later used by organized crime organizations for spamming and phishing. By 2000, these organizations had
evolved into businesses, such as CarderPlanet,< http://blogs.creditcards.com/2008/05/secret-history-of-carderplanet.php > which specialized in credit card numbers and other personally identifiable information (PII). They created forums specifically for communicating with other members of the cybercrime underworld, and behaved like corporations in dedicating personnel to specific functions of handling personal information.< http://www.crn.com/security/218800207 >

There is even an official entity called the Russian Business Network (RBN), which is based in St. Petersburg.< http://rbnexploit.blogspot.com/ > The RBN provides Web hosting services that cater exclusively to cyber criminals. According to Brian Krebs, writing in the Washington Post, "The Russian Business Network sells Web site hosting to people engaged in criminal activity, the security experts say. Groups operating through the company’s computers are thought to be responsible for about half of …[2006’s]… incidents of ‘phishing’….”< http://www.washingtonpost.com/wp-dyn/content/article/2007/10/12/AR2007101202461.html >

* * *

In the next installment, the authors discuss cyber pirates based in Asia. In the meantime, they welcome the torrents of abusive e-mail that naturally follow any mention of crime in specific geographic areas.

* * *

ABOUT THE AUTHORS

Kathleen Hayman is an analyst with the US Department of Justice, and she has been a consultant with Certico Corporation< http://www.certicoglobal.com > for three years. She can be reached at Kathleen.Hayman@gmail.com.

Michael Miora has designed and assessed secure, survivable, highly robust systems for Industry and Government over the past 30 years, and has become an internationally recognized expert in InfoSec, Business Continuity and Incident Response. Miora, one of the original professionals granted the CISSP in the 90s and the ISSMP in 2004 was accepted as a Fellow of the Business Continuity Institute< http://www.thebci.org/ > (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,< http://www.contingenz.com > a specialty consulting firm and the developers of IMCD Business Backup.< http://www.contingenz.com/IMCD > He can be reached via email at mmiora@contingenz.com or mmiora@miora.com.

Allen Forbes is currently the President of Certico Corporation< http://www.certicoglobal.com > serving large critical infrastructure providers in all matters concerning security. A 28-year veteran in the US Marine Corps and currently a member of the US Marine Corps Reserve, Forbes has served in a number of senior logistics, operations, intelligence, and security positions in both the government and private industry. He can be reached at aforbes@certicoglobal.com.

M. E. Kabay, PhD, CISSP-ISSMP < mailto:mekabay@gmail.com > specializes in security and operations management consulting services. CV online.< http://www.mekabay.com/cv/ >

Copyright © 2009 Kathleen E. Hayman, Michael Miora, Allen P. Forbes & 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.