The need for protection against cyber crime is ever increasing, especially considering the volume of personally identifiable information (PII) and financial transactions which corporations and financial institutions manage on a daily basis. Moreover, cyber crime is often a transnational threat, creating even more difficulty for law enforcement to pursue cyber criminals. The added complexities of international inconsistencies with respect to laws pertaining to PII exacerbate the problem, and current cyber crime legislation in key areas around the world currently does not permit virtual self defense.


Data protection law has been the subject of an increasing number of jurisdictional disputes, which have largely been driven by the ubiquity of the Internet, the interconnectedness of the global economy, and the growth of data protection law around the world in recent years. There are also an increasing number of instances where data protection law conflicts with legal obligations in other areas. Moreover, the rapid development of new computing techniques (such as so-called ‘cloud computing’) is putting even greater pressure on traditional jurisdictional theories. Jurisdictional uncertainties about data protection law have important implications, since they may dissuade individuals and companies from engaging in electronic commerce, can prove unsettling for individuals whose personal data are processed, and impose burdens on regulators. These difficulties are increased by the fact that, so far, there is no binding legal instrument of global application covering either jurisdiction on the Internet or data protection.

This is the first 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. The discussion is restricted to traditional crimes committed through virtual means and the implications of potential solutions. The articles address how corporations and financial institutions can conduct e-commerce in areas with minimal security and cyber law enforcement capabilities and also discuss the question of which areas and organizations are most often targets of cyber crime and which attackers pose the greatest threat to e-commerce is also discussed. The articles have been edited by M. E. Kabay, who suggested changes as well as requesting and adding supplemental references to the text.

* * *

The Piracy

On June 12, 2009, members of a transnational telephone hacking scheme were indicted in New Jersey. These individuals, many based in the Philippines, were accused of unauthorized entry into the telephone systems of major US businesses and other entities and of attempting to sell
information about these vulnerabilities to Pakistani nationals residing in Italy. The arrests and indictments were the result of a three-year investigation that included a high degree of cooperation and coordination among many affected US businesses and foreign entities.<

The most tempting, untapped markets can have significant security challenges. Perhaps the most tempting markets are those where technological pirates and privateers dominate. These are not pirates that plunder the high seas, nor are they privateers given ships and commissioned by royalty. These technological scallywags constitute very real threats to the multinational corporation. PII is a deliberate target of cyber criminals, members of criminal organizations and foreign governments. These cyber criminals obtain sensitive PII for profit. They perceive corporations as galleons—giant, slow ships filled with a vast stockpile of assets; they seek to overtake the ships to take as much as they can before being identified or captured. They vanish as suddenly as they strike using the anonymity of the Internet for mobility, masking their trails and escaping to reemerge another day in another guise.

The need for protection against cyber crime is great, especially considering the PII and financial transactions which Corporations and financial institutions manage on a daily basis. Cyber criminals, members of criminal organizations, and potentially foreign governments all specifically target PII. Cyber crime can be a transnational threat, creating even more difficulty for law.

Unless current cyber crime legislation is modified to permit virtual “self defense” against these pirates, business to business e-commerce in lawless areas is likely best conducted via Virtual Private Networks (VPNs). In areas with minimal security and law enforcement capabilities, this method of self protection is critical. Current cyber crime legislation around the world does not address virtual “self defense.” Most existing cyber crime legislation is broad, and does not yet distinguish among attacks based on intent. Unless current legislation is changed or modified, using Virtual Private Networks (VPNs) and security awareness training are likely the best option for operating in unstable areas.

Businesses, particularly those in the financial sector, are facing the challenge of ensuring self-protection within legal bounds that do not drive away their clientele. The balance between customer service and Internet security is delicate.

The Pirates and Privateers: Who are the Scallywags?

The threat is multi-layered: pirates could be acting independently or as members of larger cyber crime groups. Some, however, are privateers, wreaking havoc at the behest of foreign nations and organizations. While privateers tend to focus on governments and contractors upon which the governments rely, they still have a vested interest in draining an “enemy” economy of resources.

Pirates and privateers use different techniques for their activities. Some could select a particularly tempting company as a target, particularly if the company is experiencing changes or fluctuations that would render it vulnerable to attack. Others may pose an insider threat as disgruntled employees with access to sensitive identifying information are tempted to use the information for their own personal gain.

All pirates, however, face the question of how to transport their plunder. Cyber crime gangs may recruit both knowing and unknowing accomplices to perform simple online tasks to facilitate the transfer of their ill-gotten gains. The complexity of a cyber crime case can present a difficult

As demonstrated in the transnational telephone hacking scheme described above, a plot may involve players from around the globe. Perpetrators, end customers, and intermediates may reside in dispersed geographical and jurisdictional areas. In this example, the US was fortunate to have cooperative global law enforcement partners in the Philippines and in Italy. This may not always be the case, a dilemma which further strengthens the pirates in their coves.

* * *

In the next installment, the authors present some top-level findings and analyses about the environment or climate affecting the activities of pirates and privateers around the world.

* * *

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.