This final article in a series of four articles examines issues of defense against cyber pirates. In laws and regulations, distinctions are not made between passive defenses, such as firewalls, anti-malware and other conventional defenses, and active defenses such as counter attacks. Perhaps such distinctions are necessary.

**Ethical Defense in an Unethical Environment**

When a business operates in an environment that is lacking sufficient law enforcement strength to fight cyber crime or to provide support for victims, the business must provide its own cyber security. In some countries, criminal organizations may have infiltrated law enforcement, creating a possibly hostile law enforcement atmosphere.

Laws and regulations worldwide typically do not permit virtual, active self defense. While cyber warfare among governments can be a topic of conjecture and discussion, cyber self defense for individuals and businesses has not been discussed at the same levels or with the same general awareness. In theory, businesses could set up online electric fences to trigger counter attacks that render the attacker’s computer unable to continue the attack.

Virtual self defense, however, would not be a panacea for cyber crime. As Orin S. Kerr notes in his 2004 article, “Virtual Crime, Virtual Deterrence: A Skeptical View of Self-Help, Architecture, and Civil Liability,” in *Journal of Law, Economics & Policy*, Vol 1 (January 2005) there is a point at which this idea can no longer apply. Many hackers use multiple proxies, which complicates tracing the original source of the hack. The use of proxies raises the question of whether host networks and sites could or should be held accountable for the cyber crime activity. Since FBI Director Mueller’s request for Congress to increase regulations on ISP data retention to aid child pornography investigations in April 2008, not much else has materialized to hold ISPs and social networking sites accountable legally. ISPs and social networking sites largely remain self-regulated concerning child pornography; holding them accountable for cyber fraud activities would likely be at least as difficult.

Generally speaking, current cyber crime laws and regulations do not allow for a distinction between a cyber attack and an act of active cyber self defense. For example, the Computer Fraud and Abuse Act [18 USC 1030(a)]<http://www4.law.cornell.edu/uscode/html/uscode18/uscode18_00001030----000-.html>, the most important US law governing computer penetration, makes no mention of retaliation as an exculpation. Unless current legislation is modified, businesses must rely on more traditional IT security methods and frameworks to prevent cyber attacks. Virtual private networks (VPNs) can provide a relative level of e-commerce security, though even the best VPN can be only as secure as the entities that employ it. Therefore, businesses should exercise caution in selecting business partners and services, with a mandatory vetting of a potential partner's security practices before making a formal electronic connection.
Although VPNs may partially reduce the outside threat to a business, the insider threat remains. Security awareness training for employees is essential so they can understand how the threat appears and how identify possible insider attackers. A system should be in place in which suspicious activity can be reported easily and fairly, with reporting anonymity, while also providing a fair evaluation for the individual in question.

Fairness in evaluations is important because morale is vital to a company's security and an absolute necessity if we are to keep disgruntled employees from evolving into insider threats. In particular, the recent economic downturn adds an additional layer to the complex psychology behind the insider threat. Without memory of previous economic hardships, the employee may feel a more extreme sense of loss and hopelessness, making the employee more open to profiting from the company's vulnerabilities.

According to Carol Ko, writing in *MIS Asia*, a significant portion of the Asia-Pacific data breaches in 2008 was due to terminated employees stealing information from their organizations. [http://www.mis-asia.com/technology_centre/security/how-do-you-tackle-cyber-crime](http://www.mis-asia.com/technology_centre/security/how-do-you-tackle-cyber-crime) “Layoffs due to the effects of the global financial crisis have seen a jump in insider breaches.” Insider end user cases were often cases where employees had been terminated, but their access to critical data had not yet been removed; the insiders stolen data in the period between when they are given notice and when they exit the organization.” Revenge appears to remain a strong impetus to crime.

With apologies to the famous antivirus company [http://www.avast.com/](http://www.avast.com/): Avast, me hearties: VPNs and security awareness training are likely the only real options for operating in unstable or lawless 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](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/](http://www.thebci.org/) (FBCI) in 2005. Miora founded and currently serves as President of ContingenZ Corporation,[http://www.contingenz.com](http://www.contingenz.com) a specialty consulting firm and the developers of IMCD Business Backup.[http://www.contingenz.com/IMCD](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](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](mailto:mekabay@gmail.com) specializes in security and operations management consulting services. CV online.[http://www.mekabay.com/cv/](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.