Case Studies in Working with Law Enforcement (1):
The Consequences of Obstruction

by M. E. Kabay, PhD, CISSP-ISSMP
Associate Professor of Information Assurance
School of Business & Management
Norwich University, Northfield VT

Should we work with law enforcement when we encounter security breaches?

Michael Meline, MSIA, CISSP, CFE, CEH <http://www.linkedin.com/pub/michael-meline/b/83b/395> is a former United States Marine and a former Yuma County, Arizona Deputy Sheriff. In today’s column and the next, he presents an excellent case study centered on a credit union that he used in his master’s degree research at Norwich University <http://infoassurance.norwich.edu>. Everything that follows is entirely Mr Meline’s work with minor edits.

* * *

Some security experts think that law enforcement will leak the incident to the press and that the negative publicity will harm the organization. In the 2005 Computer Security Institute Annual Survey<http://i.cmpnet.com/goci/db_area/pdfs/fbi/FBI2005.pdf> by Lawrence A. Gordon<http://www.rhsmith.umd.edu/faculty/lgordon/>, Martin P. Loeb<http://www.rhsmith.umd.edu/faculty/mloeb/>, William Lucyshyn<http://en.scientificcommons.org/william_lucyshyn>, and Robert Richardson<http://www.gocsi.com/contact_us.jhtml>, the authors point out that “The percentage of organizations reporting computer intrusions to law enforcement has continued its multi-year decline. The key reason cited for not reporting intrusions to law enforcement is the concern for negative publicity."[p 2 in report / p 3 in PDF]

Figure 22 in the 2005 CSI report shows that the fear of negative publicity was mentioned by 43% of the 423 respondents. The other factors mentioned were as follows:

- Competitors will use the data for unfair competitive advantage (33%)
- Civil remedy seemed the best course of action (16%)
- Victimized organizations were unaware that law enforcement would be interested (16%).

My case study illustrates the importance of reporting crimes and working closely with law enforcement and it involved me personally when I was a law enforcement officer. To make the case more usable in teaching and for security awareness, the rest of the description will be in the third person.

The case began when an 80 year old woman reported to a law enforcement officer (LEO) that an unknown person had taken over $100,000.00 from her bank account. The victim stated that she had the money in her account one day, and the following day it was missing. She had not reported the missing money to the bank, just to the LEO.

The LEO went to the bank to investigate the case and was immediately met with resistance. The manager came in and stated that he would just refund the money and that an investigation would not be necessary. He stated that the bank could not stand the negative impact that the case would
have on the bank’s reputation. The LEO demanded that the manager of the bank cooperate in the investigation and told the manager that the person responsible would be held accountable for the crimes. After considerable obstruction, the bank finally assisted the officer in the investigation.

As it turned out, the teller who had her workstation next to the controls for the entire camera system was the culprit. She had a friend who had worked for the victim and who had stolen checks from the woman. When this friend arrived at the bank, the teller turned off the cameras and cashed several checks as if the victim had come in herself, even writing the victim’s driver’s license number onto the checks. The two women who were responsible were both arrested.

When interviewed, the teller stated that she had done this countless times in the past and that the bank had simply refunded the money with no real investigation. She stated that the bank had no professionals in place to prevent such an occurrence. She also stated that employees frequently committed crimes because they knew they would not be caught. It was determined that the bank had taken a great many losses. When the bank’s Board of Supervisors found out about this pattern, the manager was fired.

In the second of this two-part series, Michael Meline concludes with a description of how he improved security at a Credit Union where he was hired as security manager.

* * *

Join me online for three courses in July and August 2009 under the auspices of Security University. We will be meeting via conference call on Saturdays and Sundays for six hours each day and then for three hours in the evenings of Mon-Tue-Wed-Thu. The courses are “Introduction to IA for Non-Technical Managers,” (July 18-23)< http://www.securityuniversity.net/classes_online_Intro_Info_Assurance.php > “Management of IA,” (Aug 1-6)< http://www.securityuniversity.net/classes_online_Mgmt_Info_Assurance.php > and “Cyberlaw for IA Professionals.”(Aug 8-13)< http://www.securityuniversity.net/classes_online_Cyberlaw_IA_Professionals.php > Each course will have the lectures and discussions recorded and available for download – and there will be a dedicated discussion group online for participants to discuss points and questions. See you online!

* * *

Michael Meline, MSIA, CISSP, CFE, CEH < http://www.linkedin.com/pub/michael-meline/b/83b/395 > is President of ArizonaFIRST Coalition < http://www.arizonafirst.org/ > which is dedicated to enhancing “the ability of member institutions to respond and recover from incidents affecting the financial sector by fostering partnerships and collaboration between public sector agencies, public utilities, service providers, volunteer agencies and infrastructure providers.” The organization’s Web site has a number of valuable links for emergency preparedness on its home page. In addition, Mr Meline serves as Steering Committee Chairman at the Community Justice Boards of the Greater Yuma Area and is a member of InfraGard. He welcomes your comments.< mailto:jmmeline@beamspeed.net >

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 Michael Meline & 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.