

Hello ISSA Journal readers

It is a truism that ethics is a stronger concept than law because many more things may be legal than are ethical; but there is an important caveat to keep in mind: ethics cannot trump law. In the October 29, 2007 issue of *Computerworld*, there is an excellent article by Tam Harbert entitled “*Ethics in IT*,” in which he shares the story of Bryan, an IT director for an unnamed company. In the course of his duties, Bryan discovered a senior company employee viewing pornographic web sites in violation of security policy. This, of course, is troubling, but the more serious matter was that some of the images constituted child pornography. Bryan reported the issue to his manager who chose to take no further action beyond a brief investigation and acceptance of the employee’s explanation of how the images came to be on his computer. As most of us would agree that we have an ethical obligation to preserve the confidentiality of internal security incidents, it could be said that Bryan acted ethically in taking no further action (though the article did mention that he considered reporting the matter to the FBI).

Unfortunately, there are very serious issues here because the policy violation involved child pornography: a heinous offense universally condemned and subject to strict legal penalties in the U.S. as well as many other nations. In fact, the possession of as few as three images of child pornography is a felony under U.S. law – this is an important distinction because it criminalizes not only the production or distribution of child pornography but also its possession.

When Bryan discovered the child pornography, a number of troubling legal issues arose: Bryan now has knowledge of the probable commission of a Federal offense; and Bryan himself can be considered in “possession” of the images and therefore guilty of the same offense. Bryan, however, reported the matter to management, which absolved him of any responsibility, right?

Unfortunately, it probably does not. While definitions vary, having the knowledge of the commission of a crime without reporting the crime to law enforcement can constitute being an accessory after the fact and participating in a conspiracy to conceal the commission of a crime. Add these possible charges to the possession charge and Bryan could potentially be facing years in federal prison and lifetime registration as a sex offender. Very serious consequences for a loyal IT employee who was just “doing his job” in accordance with company policy.

What lessons can a practicing security professional draw from Bryan’s situation? First, obedience to organizational policy when it is silent in a matter constitutes a very weak defense when it involves concealing the possible commission of a crime. Policies that spell out immediate referral to law enforcement are recommended if child pornography is discovered; if items relating to legislation regarding national security are discovered; if government classified information is discovered; and/or if financial transactions are identified that could have links to terrorism. In Bryan’s situation, it is possible that a law enforcement investigation would have exonerated the employee as did the internal investigation (the child pornography may have been downloaded by a Trojan or other malware; the employee’s computer may have been compromised and an attacker had downloaded the material, etc.), but the important distinction would be that Bryan and his organization had complied with legal requirements.

Security professionals must adhere to the highest ethical standards in protecting their organization and its assets; but at the same time, those ethical standards cannot be used as a reason for not complying with the law. Bryan found himself in a very tough situation and made a choice that most of us would likely understand and find somewhat reasonable under the circumstances. That choice, however, carried risk of extremely severe consequences – do not be Bryan.

Have you faced a similar situation? Let us know – Ethics@ISSA.org.

About the Author

Richard Austin, CISSP, is a 30+ year veteran of the IT industry in positions ranging from software developer to security architect. He earned a MSc degree with a concentration in information security from Kennesaw State University, a National Center of Academic Excellence in Information Assurance Education, and serves as a part-time faculty in their CSIS department. Richard is a member of IEEE, IEEE Computer Society, ACM, CSI, HTCIA, ISACA and ISSA and frequently writes and speaks on storage networking security and digital forensics.