Buffalo Business First: The virtual reality of white-collar crimes by B. Kevin Burke

October 10, 2013 | **ARTICLES**

The task force acknowledged that the proliferation and failure of so-called “Boutique Statutes” — statutes created to address narrow slivers of criminal conduct in isolated and oftentimes highly regulated areas of the law — is a problem. It reviewed many of those statutes (e.g., health care fraud, life settlement fraud, residential mortgage fraud) and found that those statutes, typically enacted following instances of widespread public outcry (e.g., massive data breaches at Target, Best Buy, Walgreen’s, Marriott, and Nasdaq), too often go unutilized and only work to further confuse the patchwork of civil and criminal statutes governing certain activities. Thus, rather than seeking to add to the sheer number of criminal statutes, the task force suggested strengthening the “basic statutes” that are the bedrock of the criminal law (e.g., larceny, scheme to defraud).

Regarding Internet-related crime, the task force recommended treating online theft, unfair competition and fraud in the same vein as other criminal acts, extending existing laws to reflect modern circumstances. Although laptop computers, smartphones, email, flash drives and other electronic storage devices did not exist when the Bartlett Commission drafted New York’s Penal Law in 1965, the basic principles underlying the criminal law — chiefly the punishment of the criminal mind and criminal acts — remain the same. Likewise, the goals of our criminal system — punishment, rehabilitation and deterrence — remain fundamental tenets of the law. Hacking into a company’s banking information is no different than stealing money out of that company’s safe deposit box. The punishment (and related deterrent effect) should be the same.

The task force acknowledged that cybercrime is a pervasive and rapidly expanding threat, an observation bolstered by the fact that 37 percent of all felony complaints drafted by the New York County District Attorney’s Office in 2012 included charges related to identity theft or cybercrime. This criminal activity has had a measurable effect on small business. The National Small Business Association recently released its 2013 Small Business Technology Survey. Among the findings were that 94 percent of small-business owners are worried about cybersecurity and nearly half reported their businesses were victims of cyberattacks.

The task force recognized that these small-business owners have good reason to be concerned, since the largest growth area for cyberattacks in 2012 was businesses with fewer than 250 employees. In fact, 31 percent of all attacks singled out that group, a threefold increase in number from 2011. The employees most singled out for attack in 2012 — 27 percent — were knowledge workers such as engineers, scientists, lawyers and communications specialists. These people create the intellectual property that attackers want. Those in sales tasked with managing customer data were the target of 24 percent of attacks.

In response to these worrisome numbers, the task force recommended amending the Penal Law to treat computer attacks more seriously, modifying the current identify theft laws to treat identity thefts more seriously and to better

protect the most vulnerable victims of identity theft, and strengthening the law that prohibits unlawful possession of a devices designed to steal electronically stored information (ESI).

To ensure cybercrimes are treated with appropriate seriousness, the task force recommended gradating the crime of computer tampering and suggested the creation of a Class B felony for computer tampering that causes loss of $1 million or more. The task force also proposed expanding the statutory definition of “computer material,” which is presently restricted to medical records, government records or data that provides competitive advantage to the individual accessing it without permission. The task force further recommended broadening the definition of computer material found in Penal Law §156.00 (5)(c) to allow both computer trespass and computer tampering to be treated with additional seriousness.

The task force also identified weaknesses in the state’s identity theft statute, which is currently split into three degrees from Class A misdemeanor to Class D felony. The task force recommended amending the current identity theft statute to create crimes ranging from a Class A misdemeanor to a Class B felony, with thresholds triggered by the dollar amount obtained or the number of identities assumed. The task force also proposed the creating of a new Class E felony — Aggravated Identity Theft in the Second Degree — designed to protect vulnerable groups such as the elderly, the incompetent and the physically disabled.

These changes, if enacted, should provide law enforcement officials much-needed tools to better protect New York’s individuals and businesses against the increasingly sophisticated cyber criminals who threaten the citizens of this state.