available at www.sciencedirect.com

ScienceDirect

journal homepage: www.elsevier.com/locate/diin

Digital Investigation

The Digital Crime Tsunami

*Greg Gogolin**

Ferris State University, IRC 212G, 1301 South Street, Big Rapids, MI 49307, USA

ARTICLE INFO

Article history:
Received 8 April 2010
Received in revised form
21 June 2010
Accepted 15 July 2010

Keywords:
Digital crime
Cyber crime
Law enforcement digital crime investigation
Cyber crime investigation
Michigan digital crime
Michigan cyber crime
United States cyber crime
Cyber crime investigation capability
Digital crime trends
Cyber crime trends

ABSTRACT

This study examines the current level of digital crime experience and investigative capabilities of law enforcement in Michigan. Information was obtained through interviews with members of Michigan Sheriff Departments. Following the collection and analysis of data, the results were extrapolated to the national level in order to provide a picture of what is facing law enforcement at the national level. The extrapolation was supported by FBI crime reports and other information sources. The results of the study argue that law enforcement is in a dire situation when it comes to dealing with digital crime. The pace of technical change and digital/cyber crime trends when juxtaposed with law enforcement's ability to deal investigate and prosecute these crimes provides for a bleak prognosis for the law enforcement and legal system.

History is littered with stories of industries and even whole nations that collapsed because they didn't foresee or adapt to dramatic changes. The legal system is at risk of joining this auspicious list. The cause? Digital Crime. This study examines law enforcement digital crime investigation capabilities in Michigan and extrapolates those findings to the national level of the United States. While the extrapolation process may be considered an approximation, it does point out the potential for some alarming consequences.

The primary investigator conducted a partial population study of the 83 sheriff's departments in Michigan. A minimum of three attempts to contact each agency were made between March and June 2009. A total of 45 of the 83 agencies agreed to participate in the study and answered a series of 25 interview questions that were posed via telephone and recorded in an online survey instrument. The respondent typically was the sheriff or undersheriff at the smaller agencies, and detectives at the larger agencies. Some agencies declined to answer some of the questions. The majority of the agencies that were not included in the study either specifically requested to be excluded from the study or were non-responsive to attempts at contact.

While it is clear that progress has been made in investigating digital crime, it is also clear that the legal and judicial systems have little appreciation of the power of technology to influence society. This belief is not unique to Michigan. Moore's law basically states that the number of transistors placed on a chip doubles every 2 years. Advancement in storage capacity perhaps even trumps that. This translates to a continual and dramatic increase in the power of digital

* Tel.: +1 231 591 3159.
E-mail address: ismgreg@yahoo.com.
1742-2876/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
doi:10.1016/j.diin.2010.07.001

devices such as computers, cell phones and other components. This has not gone unnoticed by those with dark intentions.

Many law enforcement agencies reported during the interviews conducted that 50% or more of their cases have a digital component, and most agencies report that this number is increasing. Couple this with the fact that many digital crime labs, including the state digital crime labs in Michigan, have backlogs approaching or exceeding 2 years. This means that many cases get pled out in the court system or are not even pursued. The resources just aren't there to support the amount of work necessary to stay current with digital crimes.

In order to determine the capacity of law enforcement to investigate digital crime, one needs to know the number of crimes with a digital component; the number of cases an investigator can process per year; and the number of investigators. The FBI publishes annual crime statistics, but they do not indicate how many crimes have a digital component. However, a series of scenarios can be extrapolated from the data to make some interesting, if not provocative, conclusions.

The FBI crime statistics indicate that there were 11,149,927 reported crimes in 2008 (FBI.gov, 2009). This included 1,382,012 violent crimes and 9,767,915 property crimes. Crimes such as arson are not included in this data.

The Internet Crime Complaint Center (2009) reported that it received 336,665 complaints in 2009 involving crimes with an Internet component. This is an increase from 275,284 complaints in 2008 and 206,884 complaints in 2007. Clearly, the trend is increasing at a rapid rate. Not captured in these statistics is a common perception that they are under-reported. The implication for what is presented in this article is the potential for understating the digital crime problem.

In a digital forensic investigation, it can take 4–8 h just to make an image (forensic copy) of a typical computer, which is one of the initial steps in the digital investigation process. After the image is taken, a basic analysis can begin. A general metric is that a straight forward digital crime case involving a computer can take 40 h. That doesn't take into account common events such as unfamiliar devices, additional external storage, flash drives, encryption, incompatibilities with the forensic software and the devices being investigated – or a host of other things that can consume large blocks of time. A complex case takes well beyond 40 h. In the 2009 Michigan law enforcement study, a sample of full-time digital forensic investigators reported that they could process an average of about 35 cases/year. A cell phone forensic exam typically takes much less time that a computer exam, but the complexity and capabilities of cell phones and small devices is increasing rapidly. This may mean that the time it takes to investigate a cell phone may increase in the future, not decrease. It is also important to understand that security techniques, call and text records, as well as tower triangulation to find the approximate location of the user when a device was used, can add to the complexity of cell phone exams.

Conversation with digital investigators conducted as part of the 2009 Michigan study uncovered most of the Michigan agencies that handle digital crime investigation. This included cities such as Detroit and other municipalities that have digital crime investigation capabilities. There might be some other local agencies not identified, but since they were not known by the other agencies they most likely do not have a heavy digital crime case load. The study did not include conversations with federal agencies such as the FBI, ATF, or DEA. As such, this researcher is reasonably confident that there are approximately 70 digital crime investigators in the ranks of Michigan law enforcement (state and local). A closer investigation of the demands placed on those 70 investigators, as well as a look at how well equipped they are sheds more light on the premise of this article. While it was not apparent to this researcher at the onset of the study, it became clear that a large percentage (perhaps more than half) of the digital crime investigators work on digital cases on a part time basis. The data supporting this finding was not recorded as part of this study, but it is worth noting as a potential trend or influence.

Only 34% of the investigators received formal training in laboratory digital forensics, with the majority being trained 2 weeks or less. Senior investigators have as much as 6 weeks of formal training, and only 20% of all investigators received formal training in intrusion detection. All investigators in the study were trained in criminal justice first, and almost none of that initial training had been directed at digital investigation.

Digital skills are perishable if not kept current, yet 40% of the investigators received no annual training, and a further 35% reported receiving between 1 and 5 days of annual training. Only 15% of agencies reported having audio/video analysis capabilities.

Digital crime investigation is expensive. In addition to training, the equipment, laboratory standards, supporting infrastructure, and software licenses are a substantial undertaking. No agency in the study reported an increase in funding for digital crime investigation over the previous year. That would tend to point toward a steady state or declining capability as the norm even though all indications are that the rate of digital crime is increasing. One agency indicated that their digital crime unit was disbanded and the lead detective was laid off. Another agency indicated that their digital crime detective was assigned to non-digital crimes for over a year after being trained, and then when the detective was assigned to a digital crime case he reported that he had forgotten most of the training and the licenses for the forensic software had expired.

This researcher could find no published standard for the number of digital forensics investigators needed for a given population segment although the interviews provided insight on this topic. In this study, 47% of respondents felt that their agency was not prepared to deal with digital crime, 29% were neutral, and 24% felt that their agency was prepared to deal with digital crime. When asked the same question about the State of Michigan, 25% felt that Michigan was not prepared to deal with digital crime, 32% were neutral, and 43% felt that Michigan was prepared to deal with digital crime.

The 2008 US Census estimated that 10 million people resided in Michigan (U.S. Census Bureau, 2010). This gives a ratio of 70 digital investigators to 10 million people, or 0.7 digital investigators for 100,000 people. The same 2008 US Census figures estimate the population of the United States at 304 million. Can we assume that Michigan is representative of