INFORMATION SECURITY IN FEDERAL BUREAU OF INVESTIGATIONS

ІНФОРМАЦІЙНА БЕЗПЕКА У ФЕДЕРАЛЬНОМУ БЮРО РОЗСЛІДУВАНЬ

Партевян Артур 210 н.г. ФПФПКМ ННІПФСКМ НАВС.

Консультант з мови: старший викладач кафедри іноземних мов НАВС Харчук Наталія Ростиславівна.

Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take.

By the time of the First World War, multi-tier classification systems were used to communicate information to and from various fronts, which encouraged greater use of code making and breaking sections in diplomatic and military headquarters. In the United Kingdom this led to the creation of the Government Code and Cypher School in 1919. Encoding became more sophisticated between the wars as machines were employed to scramble and unscramble information. The volume of information shared by the Allied countries during the Second World War necessitated formal alignment of classification systems and procedural controls. An arcane range of markings evolved to indicate who could handle documents (usually officers rather than men) and where they should be stored as increasingly complex safes and storage facilities were developed. Procedures evolved to ensure documents were destroyed properly and it was the failure to follow these procedures which led to some of the greatest intelligence coups of the war (e.g. U-570). The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software, and data encryption. The availability of smaller, more

powerful and less expensive computing equipment made electronic data processing within the reach of small business and the home user. These computers quickly became interconnected through the Internet.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit. The academic disciplines of computer security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems.

The FBI's Cyber Division The FBI's reorganization of the last two years included the goal of making our cyber investigative resources more effective. In 2002, the reorganization resulted in the creation of the FBI's Cyber Division. The Cyber Division addresses cyber threats in a coordinated manner, allowing the FBI to stay technologically one step ahead of the cyber adversaries threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications. The Cyber Division also simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence, and other criminal investigations when aggressive technological investigative assistance is required. The Cyber Division will ensure that agents with specialized technology skills are focused on cyber related matters. At the Cyber Division we are taking a two-tracked approach to the problem. One avenue is identified as traditional criminal activity that has migrated to the Internet, such as Internet fraud, on-line identity theft, Internet child pornography, theft of trade secrets, and other similar crimes. The other, non-traditional approach consists of Internet-facilitated activity that did not exist prior to the establishment of computers, networks, and the World Wide Web. This encompasses "cyber terrorism," terrorist threats, foreign

intelligence operations, and criminal activity precipitated by illegal computer intrusions into U.S. computer networks, including the disruption of computer supported operations and the theft of sensitive data via the Internet. The FBI assesses the cyber-threat to the U.S. to be rapidly expanding, as the number of actors with the ability to utilize computers for illegal, harmful, and possibly devastating purposes is on the rise.

To accomplish its mission, the Cyber Division will form and maintain public/private alliances in conjunction with enhanced education and training to maximize counterterrorism, counterintelligence, and law enforcement cyber response capabilities. The FBI will also maximize the success of cyber investigations through awareness and exploitation of emerging technology.

To support this mission we are dramatically increasing our cyber training program and international investigative efforts. Consequently, specialized units are now being created at FBI Headquarters to provide training not only to FBI cyber squads, but also to the other agencies participating in existing or new cyberrelated task forces in which the FBI is a participant. This training will largely be provided to investigators in the field. A number of courses will be provided at the FBI Academy at Quantico.

A typical case will come to the FBI through the Internet Fraud Complaint Center (IFCC), In its fourth year of operation, IFCC has proven to be a very successful clearinghouse, receiving over 75,000 complaints in 2002 on crimes ranging from identity theft and computer intrusions to child pornography. If the IFCC received an intrusion report from a company in Birmingham, Alabama, we would first attempt to locate where the intrusion took place. That same company may have its servers in Minneapolis, while the intruder is routing attacks through Internet providers in California and Europe. If the servers in Minneapolis were hacked, the Minneapolis Cyber Crime Task Force would be assigned the lead on the case. The leads could start in California, but end up in Eastern Europe, Nigeria or even back to Birmingham, if an insider was involved. One of the FBI's Computer Analysis Response Teams

(CART) would be called upon to preserve computer forensic evidence, and that evidence could be forwarded to one of our new Regional Crime Forensic Labs, now located in Chicago, Dallas and San Diego. The Lab would determine the extent and duration of the intrusion, and whether the attacker came from inside or outside the company. Depending on the sophistication of the intruder, the case can be cracked in a few days or take years. Cases are routinely complex, and often involve international connections.