SECURITY POLICY FOR COMPUTERIZED RECORDS MANAGEMENT

EXECUTIVE PLANNING

BY: David D. Costa
Providence Fire Department
Providence, RI

An applied research project submitted to the National Fire Academy as part of the Executive Fire Officer Program

April 1999

Abstract

The problem that prompted this research is that during the planning phase for a new computerized records management system (RMS), the Providence Fire Department identified the need to protect both the equipment (i.e. hardware, software, cabling, etc.) that would be purchased and the data that would be stored. Personnel that will utilize the RMS need clear guidelines that delineate the proper use of the computer equipment and their responsibilities to secure the data and equipment from misuse or theft.

The purpose of this research project was to develop a security policy for the RMS that will be adopted as a General Order for the Providence Fire Department. Action research was the method utilized for this project to answer the following research questions:

1. What laws and regulations govern the storage, availability, retention, or theft of computerized Fire Department records?
2. What is the current level of computer knowledge and experience of Providence Firefighters?
3. Which Fire Department personnel need access to the RMS and what are their expectations for the use of the RMS technology?
4. What types of computer crimes and security incidents jeopardize the reliability and integrity of the RMS and the stored data?
5. What types of security measures are available to protect the RMS?

The procedures used for this research included a literature review, interviews of all key personnel involved with the RMS project, and a survey of the end users. The survey was

distributed to all officers assigned as response personnel as they will be responsible for the majority of the data entry.

The recommendations included adoption of the proposed security policy, creation of a security committee that includes representatives from the fire, police, communications, and data processing departments, and purchasing security based software that would give the RMS administrator the ability to regulate the level of access for each employee. In addition, the Providence Fire Department should review, revise and re-issue it's General Order regarding station security and assign six firefighters exclusively to carry out the required training.

TABLE OF CONTENTS

	PAGE
Abstract	2
Table of Contents	4
Introduction	5
Background and Significance	6
Literature Review	8
Procedures	17
Results	21
Table 1, Knowledge and Experience of Computer Technology	24
Table 2, Expected Access to Data	25
Table 3, Preferred Network Services	26
Discussion	31
Recommendations	35
References	38
Appendix A, Federal Computer Crime Statutes	40
Appendix B, Survey	41
Appendix C, Security Policy (Draft)	44
Appendix D, Station Security Policy	52

Introduction

In an effort to identify methods that would improve the efficiency of the Providence Fire Department, the City of Providence, Rhode Island, hired MMA Consulting Group, Inc. (MMA) to perform a complete analysis of the Fire Department organization (Costa, 1997). In MMA's 1997 report to the City of Providence, a recommendation was made to immediately plan, design, and implement a fully networked Fire Department-wide computerized records management system (RMS). That recommendation was followed and the project has progressed to the point where implementation will begin in March or April of 1999 (J. Leonard, personal communication, December 10, 1998).

The problem that prompted this research is that during the planning phase for the RMS project, the Providence Fire Department identified the need to protect both the equipment (i.e. hardware, software, cabling, etc.) that will be purchased and the data that will be stored in the computerized data base from unauthorized use or destruction. The personnel that will utilize the RMS need clear guidelines that delineate the proper use of the computer equipment and their responsibilities to secure the data and equipment from misuse, theft, security breaches, and so forth.

The purpose of this research project was to develop a security policy for the RMS that would be adopted as a General Order for the Providence Fire Department. Action research was the method utilized for this project to answer the following research questions:

1. What laws and regulations govern the storage, availability, retention, or theft of computerized Fire Department records?
2. What is the current level of computer knowledge and experience of Providence Firefighters?

3. Which Fire Department personnel need access to the RMS and what are their expectations for the use of the RMS technology?
4. What types of computer crimes and security incidents jeopardize the reliability and integrity of the RMS and the stored data?
5. What types of security measures are available to protect the RMS?

Background and Significance

The Providence Fire Department provides fire protection and other emergency services to the capital city of the State of Rhode Island. The residential population is 160,728 in an 18.5 square mile area (U.S. Department of Commerce, 1990). The daily population rises substantially, due to the large number of medical, educational, business, and State governmental workers that commute to Providence each weekday (MMA Consulting Group, Inc. [MMA], 1997).

The Providence Fire Department has a uniformed strength of 539 personnel that operate from 14 fire stations, an automotive maintenance shop, and a carpenter shop (MMA, 1997). Over a five year period, the department responded to an average of 35,000 emergency incidents, reviewed approximately 350 construction plans, conducted over 2500 smoke detector and business inspections, and investigated more than 800 structure or vehicle fires each year (Costa, 1996).

In the fall of 1996, the City of Providence contracted MMA to conduct an analysis of the status and capabilities of the Providence Fire Department (Costa, 1997). One area that was targeted was the information management system. Although the Providence Fire Department has some personal computers, the majority of the information management is completed with manual processes (MMA, 1997). “An effective and efficient record keeping system is the basis for

planning, budgeting, and risk analysis programs" (Carter and Rausch, 1994). In a department the size of Providence, manual coordination and tracking of information consumes an inordinate amount of man-hours, is inefficient, and has a negative impact on the entire department.

MMA (1997) issued a report that made several recommendations for increasing the efficiency of the Fire Department which included to immediately plan, design, and implement a fully networked Fire Department-wide computerized RMS. On December 31, 1998, the City of Providence signed a contract with HTE, Incorporated, for a computerized RMS for the fire, police, and communications departments (G. Mulcahy, personal communication, January 11, 1999). After 17 months of research, planning, and analysis, the Providence Fire Department has progressed to the point where implementation will begin in March or April of 1999 (J. Leonard, personal communication, December 10, 1998).

The Executive Planning student manual states: "In reality, implementation is a project within a project exactly like strategic planning, analysis, and acquisition" (National Fire Academy [NFA], 1995, p. 7-4). While planning for the implementation phase, the security and integrity of both the equipment (i.e. hardware, software, cabling, etc.) and the data that will be stored in the RMS was identified as a potential security risk that needed special attention (P. Rossiter, personal communication, December 9, 1998). "The challenge of managing network security is to provide the greatest possible function and the flexibility to the broadest set of users while safeguarding network assets, particularly shared data" (Dutton, 1994, p. xx).

When establishing a RMS network, employees should have written procedures that outline the parameters of using and securing the system and the policy should make it clear what sanctions may be imposed for any violation of the rules (Hayden, 1998). Current fire department security policies require fire department buildings to be secured and for fire department

personnel to deny access to the public in unauthorized areas (Providence Fire Department, General Order 56, 1988). In addition, the Providence Fire Department Rules and Regulations (1997) state: "Members of the Department shall be responsible for the safekeeping of all Department property entrusted to their care" (p. 16-1), "after all, data is just like any other company property" (Hayden, 1998, p. 140).

This research project was conducted to fulfill the requirements of the Executive Planning course at the National Fire Academy (NFA). The research directly relates to module seven of the Executive Planning student manual, *Implementation* (1995). As the Providence Fire Department embarks on the implementation phase of a new RMS, a comprehensive plan that promotes user involvement and is staunchly supported by upper management will greatly improve the chances of a successful implementation (NFA, 1995). The purpose of this research project was to develop a security policy for the RMS so that the appropriate training could be conducted during implementation.

Literature Review

What laws and regulations govern the storage, availability, retention, or theft of Fire Department records?

Federal Laws

"The Computer Fraud and Abuse Act of 1986 (it's been amended several times) is the main piece of legislation that governs most common computer crimes, although many other laws may be used to prosecute different types of computer crime" (Icone, Seger, and Von Storch,

1995, p. 16). Generally, a computer crime has violated federal law when it fits one of the following categories:

- The theft or compromise of national defense, foreign relations, atomic energy, or other restricted information.
- Involvement of computers owned by a United States Government department or agency.
- Involvement of a bank or other financial institution.
- It involves interstate or foreign communications.
- It involves people or computers in other states or countries.

Refer to appendix A for a list of applicable federal statutes.

State Laws

The State of Rhode Island has two categories of law that regulate the Providence Fire Department's new RMS. The first is administration of public records and the second is computer crime.

In general, Title 38 of the Rhode Island General Laws require all governmental agencies, fire departments included, to maintain all records of official business and provide access to *public records* for the general public.

A *public record or public records* are:

All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, computer stored data (including electronic mail messages, except specifically for any electronic mail messages of or to elected officials with or relating to those they represent and correspondence of or to elected officials in their official capacities) or other material regardless of physical

form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency (*Public Records Administration Act,* RI General Laws § 38-38-2-2 et seq., 1956).

Although the Public Records Administration Act requires that all records be maintained, the public does not have the right to view confidential medical records, reports of criminal investigations, trade secrets, and several other personal records. The Act makes it a crime to unlawfully keep, remove, alter, deface, mutilate, or destroy any *public record*, and establishes a fine of not less than $20 nor more than $500 for each offense.

The Rhode Island General Laws was specifically amended to address computer crime (*Criminal Offenses,* RI General Law § 11-52-1 et seq., 1956). The following list highlights the general categories of computer crime that are addressed by RI law:

- Access to computers for fraudulent purposes (felony).
- Intentional accesses, alteration, damage or destruction to any computer equipment, or computer data (felony).
- Theft of computer systems or computer data (theft over $500 is a felony, theft under $500 is a misdemeanor).
- Transmission of false data for the purpose of submitting a claim for payment (felony).
- Tampering with computer source documents (misdemeanor).

City Ordinances

The Ordinances of the City of Providence address public records in general, but not specifically for the fire department. The following section provides for access to public records:

(a) *Generally.* All city departments and agencies shall provide, to any public radio or television station, or newspaper of general circulation, access to all public documents.

(b) *Editing; copying.* Where it is necessary to edit public documents for the protection of privacy, the cost of such editing shall not be passed onto any group or individual requesting copies of such documents, when such group or individual would otherwise be entitled to access of such documents under state law. Said department or agency, however, may pass on reasonable costs of copying such documents to any group or individual other than those outlined above (Providence Code of Ordinances § 2-1 et seq., 1941 & Rev. 1946).

Rules and Regulations of the Providence Fire Department

"Officers of the Department shall properly prepare and promptly forward all reports through official channels to the Chief of Department unless otherwise provided for in these Rules and regulations" (Providence Fire Department, 1997, p. 28).

Members [of the Fire Department] shall treat the official business of the Department as confidential. They shall not impart to anyone, information which has been published in the orders of the Department nor permit persons, not members of the Department, to have access to, or make a transcript of, a Department record, except as follows:

(a) Under due process of law.

(b) As directed by, or with the approval of, the Chief of Department (Providence Fire Department, 1997, p. 27).

In accordance with the Rules and Regulations, the Chief of Department designated the Fire Marshal as *Keeper of Records* for all records relating to fire investigations, building inspections, plans review, and public education (J. Rattigan, personal communication, February 1, 1999). All other fire department records are in the care and custody of the Chief of Department.

The Rules and Regulations of the Providence Fire Department (1997) dedicate two chapters to the preparation and preservation of records and reports. The rules specify that records shall be kept complete, accurate, and preserved for various time frames (Chapters 27-28). The rules also delineate that: “the falsification of records, the making of misleading entries, or the willful mutilation of any Department record, book, paper, or document is strictly prohibited” (Providence Fire Department, 1997, p. 27).

“Having good information that is readily available is essential to managing a fire department of any size” (Schaenman, P., 1988, p. 129). The modern fire department requires a computerized records management system to meet current and future needs (Carter & Rausch, 1994). As the Providence Fire Department prepares to convert from traditional paper record keeping to computerized data storage, the department needs to protect both the equipment and the data that will be stored.

Hayden (1998), insists that prior to allowing any personnel access to a computer network, clearly defined rules should be written into a company handbook and users should acknowledge their understanding of the policies in writing. “You can have the best security infrastructure in the free world, but if your users aren’t aware of it and don’t think about it, you might as well not have any security at all” (p. 328).

Hayden identified common security risks to computer networks as ease of replication of data, non-audited networks, non-firewalled Internet-connected networks, viruses, TCP/IP attacks, social engineering, unaware users, unsecured computers, unsecured (not backed-up) data, non-malicious attacks, and malicious attacks. The variety of security risks makes attending to those concerns a never-ending process, not a final destination. “You will never create a

network that's entirely secure; however, you can continue to work towards closing up holes as more and newer holes are discovered" (Hayden, 1998, p. 320).

The writing of Hayden influenced this research by supporting the need to train personnel about computer security and to create a written policy that addresses the security of the computer network and the stored data. Proper training and written guidelines for computer security should help to protect the newly acquired assets for the Providence Fire Department.

There are four unforgivable sins listed by Dutton (1994), as network security risks. They are:

1. Failure to make appropriate, routine backups.
2. Using easy to guess passwords, no passwords, or not protecting passwords.
3. Failure to fully protect data by not implementing Network Operating System features.
4. Failure to train users and make them accountable for their actions (p. 3).

Dutton points out that although there has been much hype surrounding computer attacks by viruses and hackers, the media gives an unrealistic picture to most computer users. Icove, Seger, and Von Storch (1995) reported that 55% of computer crimes and security incidents are from human error, 20% from physical security problems (e.g. natural disasters, power supply, etc.), 10% are caused by dishonest employees, 9% from disgruntled employees, 4% from viruses, and only 1% to 3% were from outside attacks. "Indeed, you are more likely to have unprotected PCs stolen and many times more likely to lose valuable data through errors or faulty software, than you are to have a major loss caused by a virus" (Dutton, 1994, p. 4).

"In the 1993 Computer Crime Survey by COMSEC, 43 percent of the organizations admitted that they have security incidents at least once a month and 1 in 7 losses amounts to more than $100,000.00" (Dutton, 1994, p. 8). Many networks are being managed by end users

that are unaware of daily changes to the network, lack technical expertise, and are not attentive to security procedures. The complexity of computer networks is often overlooked by organizations. Both ignorance and inattention are causing lax security that is making numerous computer networks vulnerable to attack.

Icove et al. (1995) supported Dutton's work when they reported “The FBI’s Computer Crimes Squad estimates that between 85 and 97 percent of computer intrusions are not even detected” (p. 3). In a recent test sponsored by the Department of Defense attempts were made to attack 8932 computer systems that participated in the test. Of those systems, 7860 were successfully penetrated, 390 penetrations were detected, and only 19 of the system managers actually reported the attacks.

Dutton (1994) describes three basic methods used for securing computer networks. They are physical access safeguards, electronic network hardware and software security features, and management controls such as policies, standards, plans, systems, and procedures.

Physical controls may include physical barriers, emission zones, door lock and key cards, guard stations, server room, wiring closet, network control room, LAN cable, and secure workstations and peripherals. Controlling physical access is used to isolate network hardware from unauthorized persons, thereby preventing exploitation of network vulnerabilities.

Electronic hardware and software is used in a variety of ways to protect the network. Dutton (1994) noted that audit trails, password identification, scanning for viruses, backing up data and prevention of power surges are some of the protections that can be addressed by hardware and software. *Latches,* by Rhea International Organization Incorporated, is one type of software program that can address access issues related to securing a computer network and its’ records (SC Magazine, 1998). Although no system is perfect, the combination of several network

features would limit unauthorized access and provide for the safekeeping or rebuilding of data, should damage or theft occur (Dutton, 1994).

Management controls such as policies, standards, plans, systems, and procedures are utilized to create best practices for security. Some of the procedures that should be addressed by management controls include assigning and changing passwords, authorization of personnel to access the network, proper training, auditing employee access, conducting backups of files and procedures for maintenance. In addition, Icove et al. (1995) noted that accountability should be spelled out in policies that when a violation of the rules is found, the responsible employee should be disciplined accordingly, even if the employee claims an excuse like their password was stolen.

At a minimum, the company-wide Security Plan should cover the following elements of LAN security:

- Risk analysis should identify threats, vulnerabilities, and existing safeguards for the organization as a whole. It should address the potential for disaster and network failure from all causes including natural forces, fire, theft, accident, and equipment malfunction, hardware and software and so on.
- Backup and recovery strategy
- Contingency plan for emergencies including Disaster Recovery Plan and Continuity of Operations Plan.
- Data security review to ensure protection is adequate for the sensitivity of data stored, processed and communicated.
- Asset protection and risk management.
- Privacy of information.

- Document classification and marking.
- Records storage, retention, and distribution.
- Physical security.
- Safety (Dutton, 1994, p. 254).

Another issue raised by Dutton (1994) is who is responsible for the security plan? If your organization is large and there are many managers, one enterprise LAN manager is usually assigned as the responsible person. If there are several managers, collaboration on a common security plan and adaptation for your individual LAN needs may be necessary (Dutton, 1994).

The works of Dutton and Icove et al. influenced this research by promoting the need to pay particular attention to security threats within the organization itself. “Employees need training both in the use of the system and in taking responsibility for that system…Employees also need to be clear about the security policy of their organization” (Icove et al., 1995, p. 120). “An organization can invest millions of dollars in safeguards and still be completely vulnerable to electronic attack because one user chooses a dictionary word or common name for an easy to remember password"”(Dutton, 1994, p. 71).

Bernstein, Bhimani, Schultz, and Siegel (1996) wrote extensively on the need for developing a specific Internet security policy. The first decision that needs consideration is whether your business should be connected to the Internet at all. If a company determines that connection to the Internet creates too many problems or poses too much risk, a viable alternative is to continue to conduct business without the Internet.

Bernstein et al. (1996) warned not to offer any business services over the Internet without assessing the potential to control the security of the services. During a security assessment, a determination must be made of how an outsider would gain access to the network resources.

What would the legitimate points of entry be? Dial-up modems, dedicated business connections, or an Internet connection are some of the possibilities. The network security policy should regulate traffic across all the entry points. But beware, “Even the strongest perimeter defense can be rendered useless by a single, uncontrolled dial-up modem attached to the network” (Bernstein et al. 1996, p. 127).

The work of Bernstein, Bhimani, Schultz, and Siegel presents the idea that the Internet presents both opportunities and increased risks. A thorough investigation needs to be conducted to determine the feasibility of providing Internet services. The lack of some services is preferable to offering services that may lead to a major loss from fraudulent transactions or the potential for unauthorized access that can compromise the entire computer network.

Procedures

The procedures used to prepare this project began with a literature review at the Providence Public Library in Providence, Rhode Island in November 1998. Additional literature was reviewed within the Providence Fire Department, including the Fire Prevention Bureau, and the author's personal library.

A telephone interview was conducted with John Leonard on December 10, 1998. John Leonard is a sales representative for HTE Incorporated in Lake Mary, Florida. HTE Incorporated is the vendor that was chosen to supply the computer software to the Providence Fire Department for the new RMS. The interview was conducted to determine a timetable for the implementation of the RMS within the Providence Fire Department.

A telephone interview was conducted with George Buchanan on December 9, 1998 to inquire about implementation procedures for a new RMS. Mr. Buchanan is a fire department

employee in the City of Saint Johns, New Brunswick. Mr. Buchanan has been the computer systems administrator since 1989 and has been using HTE software.

A meeting was held with Acting Assistant Chief Gary Mulcahy on January 11, 1999. Chief Mulcahy is responsible for all budgetary and financial matters for the Providence Fire Department. Chief Mulcahy was consulted to verify that a contract had been signed with the vendor that was chosen to supply the software for the Providence Fire Department's RMS.

A personal interview was conducted with Lisa Vitullo on December 2, 1998. Lisa Vitullo is the data processing coordinator for the City of Providence. Lisa Vitullo was consulted regarding every aspect of the purchase and implementation of the new RMS.

A personal interview was conducted with Firefighter Paul Rossiter on December 9, 1998. Firefighter Rossiter is an 18-year veteran of the Providence Fire Department and he has an extensive background in computer technology and networking services. Firefighter Rossiter was consulted to provide some insight into the scope of the security problem that would be created by implementing a new computerized RMS.

A personal interview was conducted with Chief James F. Rattigan on February 1, 1999. Chief Rattigan was able to provide some background information on roles and responsibilities within the Providence Fire Department.

A personal interview was conducted with William Spencer on March 12, 1999. William Spencer is the project manager assigned to the City of Providence by HTE Incorporated and will oversee the installation of the new RMS. Mr. Spencer was consulted on several issues regarding the installation process and particular attention was given to security issues.

A survey was distributed in February 1999 to the officers of the Providence Fire Department. The survey was utilized to determine what the users expect from the records

management system, which personal need access to the computerized records, what levels of access are required, and the level of training that will be required prior to implementing the new system.

The District Chief Officers distributed the surveys to each of the 16 locations that will have computer workstations installed. A letter with the surveys asked each officer to complete the survey, then forward it through proper channels to the Fire Prevention Bureau. The population size for the sampling was all 124 officers assigned as response personnel. The sample included 84 lieutenants, 28 captains, and 12 chief officers that would be responsible for data entry and retrieval from the RMS. A total of 91 (73%) of the surveys were completed and returned.

Additional information was gathered through the surveys from the officers of the special service divisions (i.e. training, fire prevention, automotive, etc.), but because of the small number of personnel and their special needs, those responses were not included in the results. The results of the survey were entered into a Microsoft Access database for analysis.

The purpose of this research project was to develop a security policy for the RMS that will be adopted as a General Order for the Providence Fire Department. Historical research was utilized in that a literature review was conducted to determine others experiences with their transformation into a computerized RMS. In addition, action research was employed as the information gathered during this research was used to create a security policy that was submitted to the Chief of Department for adoption.

Limitations

Survey . The results of the survey are limited by the assumption that the surveys would be filled out honestly and objectively. After review of the responses to question number 2, it is

possible that some officers either misunderstood the question or they were reluctant to admit their level of computer knowledge. Some officers may have indicated that their level of computer knowledge was higher than their actual skills.

Another limitation of this research is the rapid pace at which computer technology is progressing. Comprehensive works concerning computer systems that were written just two years may be outdated to some degree. New computer viruses are created every day, hackers are becoming more sophisticated, and new computer services are expected to be online that security personnel have no experience protecting. Thus, the results of this research may be obsolete shortly after this report is published.

Definitions

FIREWALL: A computer that controls access to an Internet-connected network (Hayden, 1998, p. 397).

INTERNET: The global network of networks now used for everything from email to electronic commerce to research (Hayden, 1998, p. 399).

LAN (Local Area Network): A group of computers in a local area tied together without any routers between them (Hayden, 1998, p. 399).

PC: Personal Computer

TCP/IP: Transmission Control Protocol/Internet Protocol, a catchall term to describe the multifaceted protocol suite on which the Internet runs (Hayden, 1998, p. 405).

VIRUS: Any malicious software, which spreads by attaching itself or replicating a copy of itself to other software programs (Dutton, 1994).

Results

Answers to Research Questions

Question 1. What laws and regulations govern the storage, availability, retention, or theft of computerized Fire Department records?

Federal Laws

"The Computer Fraud and Abuse Act of 1986 (it's been amended several times) is the main piece of legislation that governs most common computer crimes, although many other laws may be used to prosecute different types of computer crime" (Icone, Seger, and Von Storch, 1995, p. 16). Generally, a computer crime has violated federal law when it fits one of the following categories:

- The theft or compromise of national defense, foreign relations, atomic energy, or other restricted information.
- Involvement of computers owned by a United States Government department or agency.
- Involvement of a bank or other financial institution.
- It involves interstate or foreign communications.
- It involves people or computers in other states or countries.

Refer to appendix A for a list of applicable federal statutes.

State Laws

The State of Rhode Island has two categories of law that regulate the Providence Fire Department's new RMS. The first is administration of public records and the second is computer crime.

In general, Title 38 of the Rhode Island General Law requires all governmental agencies, fire departments included, to maintain all records of official business and provide access to *public records* for the general public. The Act makes it a crime to unlawfully keep, remove, alter, deface, mutilate, or destroy any *public record*, and establishes a fine of not less than $20 nor more than $500 for each offense.

The Rhode Island General Laws was specifically amended to address computer crime (*Criminal Offenses,* RI General Law § 11-52-1 et seq., 1956). The following list highlights the general categories of computer crime that are addressed by Rhode Island law:

- Access to computers for fraudulent purposes (felony).
- Intentional accesses, alteration, damage or destruction to any computer equipment, or computer data (felony).
- Theft of computer systems or computer data (theft over $500 is a felony, theft under $500 is a misdemeanor).
- Transmission of false data for the purpose of submitting a claim for payment (felony).
- Tampering with computer source documents (misdemeanor).

City Ordinances

The Ordinances of the City of Providence address public records in general, but not specifically for the fire department. The following section provides for access to public records:

(a) *Generally.* All city departments and agencies shall provide, to any public radio or television station, or newspaper of general circulation, access to all public documents.

(b) *Editing; copying.* Where it is necessary to edit public documents for the protection of privacy, the cost of such editing shall not be passed onto any group or individual requesting copies of such documents, when such group or individual would otherwise be entitled to access of such documents under state law. Said department or agency, however, may pass on reasonable costs of copying such documents to any group or individual other than those outlined above (Providence Code of Ordinances § 2-1 et seq., 1941 & Rev. 1946).

Rules and Regulations of the Providence Fire Department

"Officers of the Department shall properly prepare and promptly forward all reports through official channels to the Chief of Department unless otherwise provided for in these Rules and regulations" (Providence Fire Department, 1997, p. 28).

Members [of the Fire Department] shall treat the official business of the Department as confidential. They shall not impart to anyone, information which has been published in the orders of the Department nor permit persons, not members of the Department, to have access to, or make a transcript of, a Department record, except as follows:

(c) Under due process of law.

(d) As directed by, or with the approval of, the Chief of Department (Providence Fire Department, 1997, p. 27).

The Rules and Regulations of the Providence Fire Department (1997) specify that records shall be kept complete, accurate, and preserved for various time frames (Chapters 27-28). The rules also delineate that: "the falsification of records, the making of misleading entries, or the

willful mutilation of any Department record, book, paper, or document is strictly prohibited" (Providence Fire Department, 1997, p. 27).

Question 2. What is the current level of computer knowledge and experience of Providence Firefighters?

Question two of the survey was used to classify the knowledge and experience of Providence Firefighters regarding computer technology. The categories were defined as beginner (no knowledge), novice (basic understanding of word processing, saving and deleting files), intermediate (knowledge of file management, databases, spreadsheets, system tools, basics of DOS or Windows operating system), and advanced (knowledge of DOS and Windows operating system, networking, network protocols, network security).

Table 1 indicates that the largest group of firefighters identified themselves as being novices (47.2%), while intermediates were a close second (27.4%), beginners (24.1%), and advanced (1%).

Table 1

Knowledge and Experience of Computer Technology

	Beginner	Novice	Intermediate	Advanced
Lieutenants	15	29	12	0
Captains	4	10	9	0
Chiefs	3	4	4	1
Total	22 (24.1%)	43 (47.2%)	25 (27.4%)	1 (1%)

<u>Question 3.</u> Which Fire Department personnel need access to the RMS and what are their expectations for the use of the RMS technology?

Question number three of the survey asked each officer to indicate what fire department records would be useful to their daily job tasks if they could retrieve them easily. Table 2 exhibits the responses to question number three.

Table 2

Expected Access to Data

	Lieutenants	Captains	Chief Officers	Total
Pre-fire Plans	42	18	9	69 (76%)
Inspection/Complaints	42	15	8	65 (71%)
Incident Reports	40	18	8	66 (73%)
EMS Reports	32	12	8	52 (57%)
Haz-Mat Storage	39	17	11	67 (74%)
Hazardous Conditions	46	16	9	71 (78%)
Personnel Records	30	13	7	50 (55%)
Exposure Data	46	17	7	70 (77%)
Scheduling	48	22	11	81 (89%)
Vehicle Maintenance	45	18	4	67 (74%)
Training	41	16	11	68 (75%)
Annual Statistics/Analysis	33	15	7	55 (60%)
SCBA Maintenance	30	10	3	43 (47%)
Personal Protective Equip.	31	11	7	49 (54%)
Administrative/Budgetary	6	7	4	17 (19%)

The largest number of responses (89%) indicated that scheduling information (i.e. rosters, vacations, sick time, etc.) would be beneficial, followed by hazardous conditions (78%), exposure data (77%), pre-fire plans (69%), training (75%), vehicle maintenance (74%), hazardous materials storage (74%), incident reports (73%), inspections and complaints (71%), annual statistics (60%), emergency medical reports (57%), personnel records (55%), personal protective equipment (54%), SCBA maintenance (47%), and administrative and budgetary (19%).

Question number 4 of the survey asked each officer to identify the computer network applications or services they thought would streamline their current job processes and the reasons those services would help. Table 3 displays the responses.

Table 3

Preferred Network Services

	Lieutenants	Captains	Chief Officers	Total
Fire Department E-mail	36	17	10	63 (69%)
Internet E-mail	23	13	9	45 (49%)
Internet Access	29	11	8	48 (53%)
Remote Access	41	10	8	59 (65%)
City Network	12	7	7	26 (29%)

A majority (69%) identified fire department e-mail as a desirable service and 95% of those respondents suggested improved communications as the reason. The second highest response was remote access from another building or vehicle (65%). Of those respondents, 63%

indicated they wanted access from their vehicles to acquire various information's that included pre-fire plans, fire code violations, hydrant locations, owner and occupant information, and any hazardous conditions. There were six emergency medical personnel that indicated they want access to past patient information.

The next highest response was Internet Access (53%). All of the respondents that suggested the need for Internet access intimated they could perform research on the latest techniques in firefighting, emergency medicine, or hazardous materials response. Following Internet access was Internet e-mail (49%), and the City of Providence computer network (29%).

Question 4. What types of computer crimes and security incidents jeopardize the reliability and integrity of the RMS and the stored data?

Hayden identified common security risks to computer networks as ease of replication of data, non-audited networks, non-firewalled Internet-connected networks, viruses, TCP/IP attacks, social engineering, unaware users, unsecured computers, unsecured (not backed-up) data, non-malicious attacks, and malicious attacks.

There are four unforgivable sins listed by Dutton (1994) as network security risks. They are:

1. Failure to make appropriate, routine backups.
2. Using easy to guess passwords, no passwords, or not protecting passwords.
3. Failure to fully protect data by not implementing Network Operating System features.
4. Failure to train users and make them accountable for their actions (p. 3).

Icove, Seger, and Von Storch (1995) reported that 55% of computer crimes and security incidents are from human error, 20% from physical security problems (e.g. natural disasters,

power supply, etc.), 10% are caused by dishonest employees, 9% from disgruntled employees, 4% from viruses, and only 1% to 3% were from outside attacks. “Indeed, you are more likely to have unprotected PCs stolen and many times more likely to lose valuable data through errors or faulty software, than you are to have a major loss caused by a virus” (Dutton, 1994, p. 4).

Dutton (1994) noted that the complexity of computer networks is often overlooked by organizations. Many networks are being managed by end users that are unaware of daily changes to the network, lack technical expertise, and are not attentive to security procedures. Icove et al. (1995) reported the FBI’s Computer Crimes Squad estimated that between 85 and 97 percent of computer intrusions are not detected. Ignorance and inattention cause lax security that makes computer networks vulnerable to attack.

Question 5. What types of security measures are available to protect the RMS?

Dutton (1994), described three basic methods used for securing computer networks. They are physical access safeguards, electronic network hardware and software security features, and management controls such as policies, standards, plans, systems, and procedures.

Physical controls, as defined by Dutton (1994), may include physical barriers, emission zones, door lock and key cards, guard stations, server room, wiring closet, network control room, LAN cable, and secure workstations and peripherals. Controlling physical access is used to isolate network hardware from unauthorized persons, thereby preventing exploitation of network vulnerabilities.

Electronic hardware and software is used in a variety of ways to protect the network. Dutton (1994), listed audit trails, password identification, scanning for viruses, backing up data and prevention of power surges as some of the protections that can be addressed by hardware and

software. Combining several network features can limit unauthorized access and provide for the safekeeping or rebuilding of data, should damage or theft occur.

Management controls such as policies, standards, plans, systems, and procedures can be utilized to increase the security of a computer network. Icove et al. (1995) listed procedures to be addressed by management controls that included assigning and changing passwords, limiting network access to authorized personnel only, proper training, auditing employees access, regular backups of files and procedures for maintenance. They insisted that accountability should be spelled out in policies that delineate that when a violation of the rules is found, the responsible employee shall be disciplined accordingly. "Employees need training both in the use of the system and in taking responsibility for that system…Employees also need to be clear about the security policy of their organization" (Icove et al., 1995, p. 120).

As part of the implementation process, HTE Incorporated will conduct a train-the-trainer program (W. Spencer, personal communication, March 12, 1999). HTE recommends that for a department the size of Providence, approximately six primary instructors should receive the training program, then those six instructors should train between 30 to 50 other personnel. Then the 30 to 50 trained personnel would begin training for the end users. As part of the training process, all personnel must have a complete understanding of the security policy adopted by the fire department (see Appendix C for proposed security policy).

Bernstein et al. (1996), characterized a "good password" as at least eight characters long; a mix of letters, numbers, and symbols; having upper and lower case letters, does not form a word, does not link a word to a common series of numbers; may be a combination of two words separated by a symbol; or may be an acronym for a common phrase. "An organization can invest millions of dollars in safeguards and still be completely vulnerable to electronic attack because

one user chooses a dictionary word or common name for an easy to remember password" (Dutton, 1994, p. 71).

Bernstein et al. (1996), warned not to offer any business services over the Internet without assessing the potential to control the security of the services. The network security policy should regulate traffic across all the entry points. "The most conservative (and thus probably the best) gateway policy in most business environments is to deny any Internet connection that is not specifically permitted" (p. 108).

Unauthorized modem access or dial-up access using either Serial Line Internet protocol (SLIP) or Point-to-Point protocol (PPP) may allow invaders a back door into the network. In the context of the Internet, a firewall is a computer with specific software that will control damage and protect a network in the event of an Internet intrusion (Bernstein et al., 1996). But, the firewall does not protect against internal threats.

Computer viruses can spread rapidly throughout a computer network, so users must take every precaution to avoid introducing one and they must be held accountable if they do (Dutton, 1994). According to Dutton, to avoid introduction of computer viruses, questionable diskettes should be scanned with anti-virus software prior to use on a network workstation. If computer viruses are a recurring problem, removal of floppy drives from workstations should eliminate the majority of problems with computer viruses (G. Buchanan, personal communication, December 9, 1998).

At a minimum, the company-wide Security Plan should cover the following elements of LAN security:

- Risk analysis should identify threats, vulnerabilities, and existing safeguards for the organization as a whole. It should address the potential for disaster and network failure

from all causes including natural forces, fire, theft, accident, and equipment malfunction, hardware and software and so on.

- Backup and recovery strategy
- Contingency plan for emergencies including Disaster Recovery Plan and Continuity of Operations Plan.
- Data security review to ensure protection is adequate for the sensitivity of data stored, processed and communicated.
- Asset protection and risk management.
- Privacy of information.
- Document classification and marking.
- Records storage, retention, and distribution.
- Physical security.
- Safety (Dutton, 1994, p. 254).

The variety of security risks makes attending to those concerns a never-ending process, not a final destination. “You will never create a network that’s entirely secure; however, you can continue to work towards closing up holes as more and newer holes are discovered” (Hayden, 1998, p. 320).

Discussion

The problem that prompted this research was that during the planning phase for the RMS project, the Providence Fire Department identified the need to protect both the equipment (i.e. hardware, software, cabling, etc.) that would be purchased and the data that would be stored in the computerized data base. “The challenge of managing network security is

to provide the greatest possible function and the flexibility to the broadest set of users while safeguarding network assets, particularly shared data" (Dutton, 1994, p. xx). Although there was a myriad of security risks that needed to be addressed, this research identified numerous opportunities to provide reasonable protection for the newly acquired assets.

Before a security policy was developed, personnel had to be identified that needed access to the RMS. "Officers of the Department shall properly prepare and promptly forward all reports through official channels to the Chief of Department unless otherwise provided for in the Rules and Regulations" (Providence Fire Department, 1997, p. 28). This passage clearly places the responsibility on all officers for data entry, with few exceptions. Taken at face value, it appears that access to the RMS could be limited exclusively to fire department officers. But, as a matter of department policy, any firefighter may be acting in the capacity of an officer on any given day dependent upon personnel availability (G. Mulcahy, personal communication, January 11, 1999). As such, virtually all fire department personnel need to have access to the RMS for data entry.

The other end of the RMS spectrum is data retrieval. Referring back to Table 2, it is clear that with the exception of SCBA maintenance and Administrative/Budgetary data, a majority of the fire officers expect to have access to all data stored in the RMS.

> The question of who has access to the management information system may well depend on the types of data involved. For example, the medical history of individuals would be closely held for privacy, and the status of an arson investigation would be closely held for security. But fire incident data might be accessible to virtually anyone (Schaenman, 1988, p.147).

In an effort to increase awareness and communication throughout the fire department, most data should be viewable by all officers of the department. The exceptions should be for

sensitive personnel matters, any type of investigations, and personal medical information. Security based software can be purchased that would give the RMS administrator the ability to regulate the level of access for each employee, thereby allowing access to personal information by an individual employee, yet preventing access to everyone else (W. Spencer, personal communication, March 12, 1999). In addition, the security software would allow the disabling of floppy disk drives and CD-ROMs to curb the introduction of viruses into the computer network yet allow the RMS administrator to utilize CD-ROMs for maintenance purposes.

Another issue where additional study is needed is how much access should rescue personnel have to past patient information? Referring back to the results of research question number three, six rescue officers indicated they need patient information garnered during previous responses to be used for patient diagnosis. While the rescue officers motives are in the best interest of the patient, allowing access to medical information poses a confidentiality problem and a potential security problem.

Confidentiality of medical information must be guarded with the utmost care. Medical records were specifically exempted from the designation of a public record in state law (*Public Records Administration Act,* RI General Law's § 38-38-2-2 et seq., 1956). This exemption curtails unlimited access to medical records and would require permission by the patient or a good faith belief that the information is necessary for diagnosis or treatment of the individual patient prior to reviewing the patients past history (*Confidentiality of Health Care Information Act,* RI General Laws § 5-37.2-4 et seq., 1956). In order to provide access to the medical records, rescue officers would need unlimited access to every medical record on file. The RMS administrator would be burdened with the task of running regular audits and review to insure only pertinent records were viewed.

Once the decision is made regarding whom has access to the RMS, security features must be implemented to safeguard the system and its' data. Dutton (1994) describes three basic methods used for securing computer networks. They are physical access safeguards, electronic network hardware and software security features, and management controls such as policies, standards, plans, systems, and procedures.

Physical access safeguards should be addressed by reemphasizing current fire department security policies that require fire department buildings to be secured and for fire department personnel to deny access to the public in unauthorized areas (Providence Fire Department, General Order 56, 1988). Additional safeguards can be taken by insuring the buildings that house the computer equipment are adequately protected by fire and security alarm systems.

Although the software for the new RMS will have several built in security features, *Latches* by Rhea International Organization Incorporated, is one software program that can address all the access issues related to securing the RMS (W. Spencer, personal communication, March 12, 1999). *Latches* is capable of checking passwords to insure they are not easily guessed and they are changed regularly, it can audit the use of each workstation, it can deny access to unauthorized users, and it is virtually impenetrable by hackers or thieves. *Latches* or a similar product would be a wise investment to provide a reasonable level of security for the RMS.

The third area to be addressed is the management controls such as policies, standards, plans, systems, and procedures. As part of the management controls, someone has to be identified as having the responsibility to implement and monitor all the security features that are instituted. "If your organization is so large that there are many managers, the Enterprise LAN manager is usually the responsible person. If there are several managers, you might collaborate

on a common security plan and adapt it for your individual LAN needs if necessary" (Dutton, 1994, p. 255).

In an effort to promote communication between the different public safety departments and to insure their security needs are addressed, a security committee could be formed that would be responsible to work together on policies and to investigate new techniques, software or hardware that may provide increased security. Committee meetings would provide a forum to discuss any problems that are discovered related to access or lack of access to the RMS, and to review any aspect related to security of the RMS. In addition, the personnel office is hiring a network engineer that will be responsible for the administration of the RMS (L. Vitullo, personal communication, December 2, 1998). The new network engineer will be responsible for security of the RMS, including, but not limited to auditing system usage, backup and recovery strategies, and implementing all software security features.

The purpose of this research project was to develop a security policy for the RMS that would be adopted as a General Order for the Providence Fire Department. Once developed and prior to any use of the RMS, training in the proper use of the software, hardware, data, and its' security features is imperative. "You can have the best security infrastructure in the free world, but if your users aren't aware of it and don't think about it, you might as well not have any security at all" (Hayden, 1998, p. 328).

Recommendations

The results of this research indicate that there are several steps that can be taken by the Providence Fire Department to ease the transition to a computerized records management system while safeguarding the integrity of the new RMS. While much of the information and procedures

reported in this research are crucial to the overall RMS project and the entire City-wide computer network, the purpose of this research was to develop a security policy for the Providence Fire Department.

The first step and crucial recommendation would be to adopt the proposed security policy as a General Order for the Providence Fire Department (see Appendix C).

In an effort to keep the security policy current, I recommend that a security committee be formed that includes representatives from the fire, police, communications, and data processing departments. The security committee would be responsible to investigate any breaches in security, new security techniques, and any hardware or software that may provide for an increase in the level of security. Security committee meetings would provide a forum to discuss any problems that are discovered related to access or lack of access to the RMS, and to review any aspect related to security of the RMS. In addition, the security committee should investigate the feasibility of providing Internet access to Fire Department personnel.

Security based software should be purchased that would give the RMS administrator the ability to regulate the level of access for each employee, thereby allowing access to personal information by an individual employee, yet preventing access to everyone else. This software should be capable of permanently disabling computers hard drives should a theft occur, thereby eliminating any possibility of a breach of confidential records.

The Providence Fire Department should review, revise and re-issue General Order 56, 1988 regarding station security to protect the computer equipment that will be installed in all fire department buildings (See Appendix D).

The Providence Fire Department should assign six firefighters exclusively to carry out the required training. A strong commitment to training will insure a smooth transition to the

computerized records management system. As part of the training and prior to issuance of a login name and password, all end users should be required to sign an affidavit stating they have reviewed and understand the security policy of the department.

References

Bernstein, T., Bhimani, A. B., Schultz, E., & Siegel, C. (1996). *Internet Security for Business.* New York, NY: John Wiley & Sons, Inc.

Carter, H. R., & Rausch, E. (1994). *Management in the Fire Service (2nd ed.).* Quincy, MA: National Fire Protection Association.

Collective Bargaining Agreement Between the City of Providence and Providence Firefighters Local 799, International Association of Firefighters, effective July 1, 1996 to June 30, 1999. (Available from City Clerk, City Hall, Providence, RI, 02903).

Confidentiality of Health Care Information Act, RI General Laws § 5-37.2-4 et seq., (1956).

Costa, D. (1996). *Providence Fire Department: Analysis of the Fire Prevention Division.* Providence, RI: Providence Fire Department.

Costa, D. (1997). *Perceptional Barriers of Providence Firefighters Towards Career Opportunities in Fire Prevention.* Providence, RI: Author.

Criminal Offenses, RI General Laws § 11-52-1 et seq., (1956).

Dutton, E. (1994). *LAN Security Handbook.* New York, NY: M & T Books.

Hayden, M. (1998). *Teach Yourself Networking in 24 Hours*. Indianapolis, IN: Sams' Publishing.

Icove, D., Seger, K., & Von Storch, W. (1995). *Computer Crime, A Crimefighter's Handbook.* Sebastopol, CA: O'Reilly & Associates, Inc.

MMA Consulting Group, Inc. (1997, May). *Providence, Rhode Island Fire Department Study.* Boston, MA: Author

National Fire Academy. (1995). *Executive Planning* (student manual). Emmitsburg, MD: Author.

Providence Code of Ordinances, *Access to Public Records* § 2-1 et seq., (1941 & Rev. 1946).

Providence Fire Department, (1988). *General Order 56: Regulations Governing Fire Department Communications, Response to Alarms, Communications Systems and Station Security*. Providence, RI: Author

Providence Fire Department, (1997). *Providence Fire Department Rules and Regulations.* Providence, RI: Author

Public Records Administration Act. RI General Laws § 38-38-2-2 et seq. (1956).

SC Magazine (July 1998). *Security on the Road.* [On-Line]. Available: http:/www.infosecnews.com/scmagazine.

Schaenman, P. (1988). *Managing Fire Services (2nd ed.)* (Coleman, R. J., & Granito, J. A., Eds.).Washington, DC: International City Management Association.

U.S. Department of Commerce (1990). *Census of population, social and economic characteristics, urban areas.* Washington, DC: U.S. Government Printing Office.

Appendix A

Federal Computer Crime Statutes from the United States Code (USC)

Title	Chapter	Section	Description
15 USC Credit Card Fraud	41	1644	Credit Card Fraud
17 USC Copyrights	1	101	Definitions
	1	102	Copyrights
	1	117	Computer Programs
	5	501	Copyrights
18 USC Crimes and Criminal Procedures	5	81	Arson
	31	641	Embezzling/Records Theft
	31	659	Embezzling/Property Fraud
	37	793	Gathering, Transmitting, or Losing Defense Information
	47	1001	Fraud/False Statements
	47	1029	Fraud/Computer or Communications

APPENDIX B

COMPUTERIZED RECORDS MANAGEMENT

SURVEY QUESTIONNAIRE

The entire Department of Public Safety is in the process of replacing and expanding their computerized records management system. Although the fire department has a limited number of personal computers, as part of the project, every fire department building will be networked to the computerized records management system.

As the RMS is installed over the next year, the majority of the fire departments records will be stored and transported electronically. With this new technology, comes an additional responsibility to provide security for the physical hardware, the computer software, and the data that is in the custody of the fire department. The greatest challenge will be to manage network security to protect the fire departments property while providing the greatest possible function and flexibility to the many users of the system.

The purpose of this survey is to determine what users expect from the records management system, who needs access to the computerized records, what levels of access are required, and the level of training that will be required prior to implementing the new system. Please check off or fill in the appropriate response, and return this survey to the Fire Prevention Bureau by February 22, 1999:

1. Check off your current rank.

____ Lieutenant

____ Captain

____ Chief

____ Other _____

____ Special service _____

***** Please specify if you are assigned to a special service division (EMS, Training, etc.)

2. How would you classify your knowledge and experience of computer technology?

____ Beginner (no knowledge)

____ Novice (basic understanding of word processing, saving and deleting files, etc.)

____ Intermediate (knowledge of file management, databases, spreadsheets, system tools, basics of DOS or Windows operating system, etc.)

____ Advanced (knowledge of DOS and Windows operating system, networking, network protocols, network security, etc.)

3. Check off the following records that would be useful to your daily job tasks if you could retrieve them easily.

____ Pre-fire plans

____ Inspection reports/complaints

____ Incident reports

____ EMS reports

____ Haz-Mat storage

____ Hazardous conditions

____ Personnel records

____ Exposure data

____ Other _____

____ Scheduling (rosters, vacations, etc.)

____ Vehicle maintenance

____ Training completed/scheduling

____ Annual run statistics/run analysis

____ SCBA maintenance

____ Personal protective equipment

____ Administrative/budgetary

4. What computer network applications or services would streamline your current job processes?

____ E-mail (fire department network only)

Why?_____

____ E-mail (internet capable)

Why?_____

____ Internet access

Why?_____

____ Remote access (from another building, vehicle, etc.)

Why?_____

____ Access to records of other city departments

Why?_____

____ Other _____

Why?_____

* NAME (OPTIONAL): _____

APPENDIX C

GENERAL ORDER **DRAFT**

TO: ALL MEMBERS OF THE DEPARTMENT

With the installation an implementation of the computer records management system (RMS) comes new responsibilities for the security and safeguarding of Fire Department records, data, and computer network assets. This General Order is promulgated to address these new responsibilities.

Federal Laws

The Computer Fraud and Abuse Act of 1986 is the Federal Legislation that governs most computer crimes, although other laws may be used to prosecute various types of computer crime. Generally, a computer crime has violated federal law when it fits one of the following categories:

- The theft or compromise of national defense, foreign relations, atomic energy, or other restricted information.
- Involvement of computers owned by a United States Government department or agency.
- Involvement of a bank or other financial institution.
- It involves interstate or foreign communications.
- It involves people or computers in other states or countries.

State Laws

The State of Rhode Island has two categories of law that regulate the Providence Fire Department's new RMS. The first is administration of public records and the second is computer crime.

In general, Title 38 of the RI General Law requires all governmental agencies, fire departments included, to maintain all records of official business and provide access to *public records* for the general public.

A *public record or public records* are:

> All documents, papers, letters, maps, books, tapes, photographs, films, sound recordings, magnetic or other tapes, electronic data processing records, computer stored data (including electronic mail messages, except specifically for any electronic mail messages of or to elected officials with or relating to those they represent and correspondence of or to elected officials in their official capacities) or other material regardless of physical form or characteristics made or received pursuant to law or ordinance or in connection with the transaction of official business by any agency (*Public Records Administration Act,* RI General Laws § 38-38-2-2 et seq., 1956).

Although the Public Records Administration Act requires that all records be maintained, the public does not have the right to view confidential medical records, reports of criminal investigations, trade secrets, and several other personal records. The Act makes it a crime to unlawfully keep, remove, alter, deface, mutilate, or destroy any *public record*, and establishes a fine of not less than $20 nor more than $500 for each offense.
The RI General Law was specifically amended to address computer crime (*Criminal Offenses,* RI General Law § 11-52-1 et seq., 1956). The following list highlights the general categories of computer crime that are addressed by RI law:

- Access to computers for fraudulent purposes (felony).
- Intentional accesses, alteration, damage or destruction to any computer equipment, or computer data (felony).
- Theft of computer systems or computer data (theft over $500 is a felony, theft under $500 is a misdemeanor).
- Transmission of false data for the purpose of submitting a claim for payment (felony).
- Tampering with computer source documents (misdemeanor).

City Ordinances

The ordinances of the City of Providence address public records in general, but not specifically for the fire department. The following section provides for access to public records:

> (a) *Generally.* All city departments and agencies shall provide, to any public radio or television station, or newspaper of general circulation, access to all public documents.
> (b) *Editing; copying.* Where it is necessary to edit public documents for the protection of privacy, the cost of such editing shall not be passed onto any group or individual requesting copies of such documents, when such group or individual would otherwise be entitled to access of such documents under state law. Said department or agency, however, may pass on reasonable costs of copying such documents to any group or individual other than those outlined above (Providence Code of Ordinances § 2-1 et seq., 1941 & Rev. 1946).

Rules and Regulations

"Officers of the Department shall properly prepare and promptly forward all reports through official channels to the Chief of Department unless otherwise provided for in these Rules and regulations" (Providence Fire Department, 1997, p. 28).

> Members [of the Fire Department] shall treat the official business of the Department as confidential. They shall not impart to anyone, information which has been published in the orders of the Department nor permit persons, not members of the Department, to have access to, or make a transcript of, a Department record, except as follows:
>
> (e) Under due process of law.
>
> (f) As directed by, or with the approval of, the Chief of Department.

In accordance with the Rules and Regulations, the Chief of Department designated the Fire Marshal as *Keeper of Records* for all records relating to fire investigations, building inspections, plan review, and public education. All other fire department records are in the care and custody of the Chief of Department.

The Rules and Regulations of the Providence Fire Department dedicate two chapters to the preparation and preservation of records and reports. The rules specify that records shall be kept complete, accurate, and preserved for various time frames. The rules also delineate that: "the falsification of records, the making of misleading entries, or the willful mutilation of any Department record, book, paper, or document is strictly prohibited" (p. 27). With the introduction of the computerized records management system, all computer records will be governed by the previous sections of the Rules and Regulations, and all Federal, State, and City Ordinances that apply, and this General Order.

Computer and Network Rules

Definitions

Account:	A record or registration of an authorized user of a computer system or computer network. An account will be identifiable to an individual by use of user identification (ID) and a password.
Authorized agent:	System Manager or System Administrator.
Authorized User:	Fire Department personnel that understand the potential threats to computer network security, his or her role in safeguarding computer network assets, has signed an agreement to abide by this General Order, and has been assigned a user identification and password.
Logic Bomb:	A type of computer virus.
Owner:	The City of Providence Fire Department (PFD).
Time Bomb:	A type of computer virus.
Trojan Horse:	A type of computer virus.
Virus:	Any malicious software, which spreads by attaching itself or replicating a copy of itself to other software programs.
Worm:	A type of computer virus.

Employee Safety

Employee safety is an important security and management responsibility. Employee stress is an increasingly important safety-related issue. Stressed, unhappy employees have more accidents and make more errors than well employees. Officers should take more than a passing interest in employee physical and mental health. Computers and computer networks will make it so easy to be highly productive that many may tend to overdue it. Long periods of time spent at the workstation keyboard can result in a number of ailments including Carpal Tunnel syndrome, eye diseases, eyestrain and headache, neck strain, and back strain. Frequent breaks from desktop computers and overall good physical fitness help to prevent a number of computer user stress-related disorders.

Carpal Tunnel syndrome is caused by repetitive wrist and hand movements and is best prevented by taking breaks away from the computer and by using wrist supports at the keyboard. When the pain of Carpal Tunnel does strike it can sometimes be alleviated by wrist bandages that provide support.

Carrying PCs, printers, and other heavy office equipment around may cause back strain. LAN and microcomputer support staff are highly susceptible to this problem since they often move equipment. A person with good muscle tone may be able to move a PC or two with no adverse physical effect whereas a person with poor muscle tone may bend over slightly and wind up in traction for a month. Use your common sense and, unless you are in excellent, well-exercised physical condition, do not even consider moving heavy equipment around.

Taking work breaks and looking out of doors, into the distance if possible can alleviate eye problems caused by the absence of natural light. This lets natural light into the eyes and exercises the eyes at the same time.

Neck and back strain may be caused in part by long hours at the keyboard, uncomfortable chairs, or poorly designed office layouts. If employees have to strain to see a screen, they should discuss the problem with the system manager. Sometimes a small adjustment can prevent a major health problem. In general, desktop computers seem well placed for tall people because they are able to maintain a natural head position while viewing the screen. Short people can have difficulty finding a comfortable working position in traditional office settings. Alternatives may be needed.

Prohibited Conduct

The following is prohibited conduct for any individual using Providence Fire Department (PFD) or City of Providence (City) managed computers or networks:

1. Use of any PFD or City computer system or computer network for illegal purposes. This shall include, but not be limited to, accessing, downloading, or copying pornographic files, using pirated software, or using unauthorized routes (such as dial-up access) to access PFD or City computer systems.

2. Use of a computer system or computer network in violation of PFD Rules and Regulations.

3. Possession, keeping or use of PFD or City property without authorization.

4. Theft of PFD property, City property or the property of any person.

5. Possession or keeping of computer software or data without authorization.

6. Unauthorized copying or use of computer software or data and unauthorized use of data processing equipment.

    a. Copying, using or causing to be copied or used computer software or data and/or using or causing to be used computer accounts and data processing equipment without authorization.

    b. Placing or causing to be placed into public locations proprietary computer software in any form unless specifically allowed by its owner. Such locations include but are not limited to file servers, non-private computer files or folders and computer bulletin boards.

7. Unauthorized use of computer and computer-related property.

    a. No person shall knowingly gain access to, attempt to gain access to, or cause access to be gained to any PFD or City computer, computer system, computer network, information storage media, or peripheral equipment, without the consent of the manager or administrator of the computer, computer system, computer network, information storage media, or peripheral equipment, or other person authorized to give consent by the owner.

    b. No person shall knowingly alter, delete, or destroy data, information, or programmatic instructions contained on or in a computer, computer system, computer network, information storage media, or peripheral equipment, without the consent of the manager or administrator of the computer, computer system, computer network, information storage media, or peripheral equipment or other person authorized to give consent by the owner.

    c. No person shall knowingly introduce a set of instructions, programmatic or otherwise into a computer, computer system, computer network, information storage media, or peripheral equipment, that will cause a computer, computer system, computer network, information storage media, or peripheral equipment to do things unwanted by the owners thereof.

    d. No person shall create, on PFD premises, or using property belonging to the PFD, a set of instructions, programmatic or otherwise, that will cause a computer, computer system, computer network, information storage media, or peripheral equipment to do things unwanted by the owners thereof.

Examples of a, b, c and d include, but are not limited to, computer "viruses," "Trojan horses," "time bombs," "logic bombs," and "worms

8. Theft of telephone or communication service or publication of any information to facilitate unauthorized access to or theft of telephone or communication services.

9. Sexual harassment, including all forms of sexual harassment (see PFD sexual harassment policy).

10. Racial harassment, including all forms of racial harassment.

11. Attempting to circumvent any PFD or City computer system or computer network security systems, or using PFD computer systems or computer networks in attempting to circumvent security systems elsewhere.

12. Failure to follow regulations of the United States government when reaching international locations by way of a computer network.

13. Accessing, modifying, or deleting any other person's computer software or data on any computer system or computer network without their permission, or storing computer software or data in another person's assigned storage space. Attempting to access, modify, or delete any other person's computer software or data on any computer system or computer network without their permission, or storing computer software or data in another person's assigned storage space except for instructors accessing computers for which appropriate access authority has been provided.

14. Failure to respect all copyrights or proprietary rights in computer software or data.

15. Unauthorized connecting, disconnecting, tampering with or make changes to any physical components of a PFD or City computer system or computer network. No person shall knowingly connect, disconnect, tamper with or make changes to any physical components of a PFD or City computer system or computer network unless the owner or authorized agent has granted their permission (e.g. external floppy drives, zip drives, CD-ROM's, modems, etc.).

16. Failure to abide by computer software contracts. When using PFD or City computer systems or computer networks, each person must abide by the PFD and City computer software contracts. Copies of contracts administered by the PFD are available through Headquarters.

17. Unauthorized attempts to access administrative data on any PFD or City computer system or computer network. Examples of administrative data include, but are not limited to, payroll information, personnel files, medical records, etc.

18. Unauthorized possession of PFD or City computer system components or computer network components at any time, and in any location, is prohibited.

19. Use of a computer system or computer network to eavesdrop, or to collect passwords or authentication information. No person shall use a PFD or City computer system or computer network to eavesdrop on another, or to collect passwords or other authentication information.

20. Forging electronic mail or other messages. No person may send a message in such a way that it appears to be sent by another person.

21. Anonymous use, or use of pseudonyms on a computer system or computer network to escape responsibility. No person shall use a computer system or computer network anonymously or use pseudonyms to attempt to escape from prosecution of laws or regulations, or otherwise to escape responsibility for their actions.

22. Use of a computer by unauthorized persons. Use of a PFD or City computer without authorization or after employment has terminated is strictly prohibited.

23. Computer or computer network harassment. Making obscene, threatening or harassing messages on a PFD or City computer or computer network. If a person requests that computer or computer network communications directed specifically to them, from a specific person cease, the latter person must stop such communications. Persisting with such contact after notification is harassment and is a violation of this and other PFD policies.

24. Failure to protect the confidentiality and privacy of computer data. When accessing administrative (or other) computer data, failure to take care to protect the confidentiality of the information, or to respect the privacy of the individuals to whom the information refers.

25. Use of a PFD or City computer account, computer system or computer network to access resources and facilities other than for bona fide PFD administrative, research, instructional, or other official business.

26. Use of PFD or City computer system or computer network resources for purely personal gain. (Monetary gains for business purposes not related to PFD business, etc.).

27. Divulging a PFD or City computer or computer network password to anyone other than the person to whom the password is assigned.

28. Failure to keep a computer account password secret. Failure to keep a computer account password secret, including failure to choose passwords which are not easy to guess, such as family names, pet names, phone numbers, addresses, social security numbers, license plate numbers, account names, user ID's, payroll numbers, information in their computer directory, or any of the above spelled backwards or otherwise trivially changed, etc., and failure to ensure no one is observing when entering a password into a machine or when a password is displayed on a screen. (This shall include writing passwords down in easily accessible areas [e.g. under keyboards, desks, etc.])

29. Failure of any authorized user of a computer to notify the system manager or administrator if the user suspects anyone else has used their account.

30. Providing either computer software or data containing passwords to another.

31. Failure of an authorized user to change his or her computer password immediately if he or she believes someone else knows his or her password.

32. Allowing anyone (even family or a supervisor for whom you work, etc.) other than the owner of a PFD computer account to use the account, except PFD or City authorized consultants when they are assisting the owner.

33. Wasteful or extravagant use of PFD or City computer system or computer network resources is prohibited.

34. Originating or propagating chain letters originated, or intentionally or knowingly propagated from PFD or City property.

35. Playing games while using PFD or City computer systems or modems. Playing games is not permitted while using any PFD or City computer system or modem. Games in this context may be defined as any computer software whose use is primarily for entertainment (exception: during initial training of personnel that have no background in computer operation).

Any member of the Providence Fire Department that witnesses a suspicious event or suspects that a violation of this General Order has occurred shall immediately report the incident to their supervisor. If their supervisor is the person suspected of breaching this security policy, then the member shall report the incident to the system administrator.

Diskettes which contain software or files from personal computers (PC's) outside the PFD must be "scanned" for viruses at authorized stand-alone PC's before the diskette is used on a network workstation.

Audit software will be used to identify unauthorized access attempts and other security violations or unusual occurrences. Users will be held accountable for security breaches.

The Providence Fire Department Rules and Regulations, along with the Collective Bargaining Agreement between the City of Providence and Providence Firefighters Local 799, identify the rights and responsibilities of members of the Providence Fire Department, and discusses the sanctions which pertain to violations of the rules and regulations.

Appendix D

PROVIDENCE FIRE DEPARTMENT

GENERAL ORDER NO. 56 SERIES 1988 19 SEPT 1988

REGULATION GOVERNING FIRE DEPARTMENT COMMUNICATIONS, RESPONSE TO ALARMS, COMMUNICATION SYSTEMS AND STATION SECURITY.

Effective this date, the following regulations, in addition to existing Rules and Regulations, are hereby established and promulgated in order to ensure proper receipt, verification of alarms and response thereto; the proper and effective handling of communication systems and operations to ensure the proper and effective response to the public and to ensure station security;

1. The officer in command of each company of the Department shall ensure that acknowledgement, verification and response to alarms; proper use of the Department telephone as prescrived in Chapter 13 of the Rules and Regulations of the Fire Department; and the receipt, preparation and processing of proper and required reports and communications continue in accordance with Fire Department Rules and Regulations, General Orders and Memoranda.

2. Members of the Department assigned to duty in any unit of the Department shall, at all times, observe the operation of alarm devices installed in such quarters, and whenever the same, shall operate defectively or transmit any incomplete, unexplained or undecipherable signal, said members shall properly communicate such fact to the officer in command of his unit, who shall, in turn, immediately notify the Dispatcher Lieutenant on duty at the Bureau of Operational Control.

3. It shall be the duty of the on duty officer in command and each on duty member assigned to each unit to decode accurately, any signal or message that involves their unit in the transmission of alarms or intelligence to the Department, and to operate the station overhead doors and other necessary devices to ensure the proper and expeditious response to alarms and emergencies.

4. The officer in command shall ensure that all signals, notifications, messages and other necessary information pertaining to the operations of his company and the Department as it relates to his company are properly recorded in the company journal in a neat, accurate and concise manner and are further communicated to all members of his company.

5. All members of each unit of the department shall be familiar with all signals, codes, and other communications as set forth in the General Orders, Memoranda and Rules and Regulations of the Fire Department.

6. The officer in command of each unit of the Department shall ensure that all Department telephone calls intended for their quarters are properly answered in the prescribed manner and shall ensure that unnecessry and unauthorized use of the Department telephone is strictly prohibited.

7. The officer in command on duty in each unit of the Fire Department shall ensure that members of his unit promptly acknowledge on the "Acknowledgement Lever" notifications, received that pertain to the operations of his company and to the department as it relates to his company.

8. Members shall:

   a. Not tamper with any fire alarms or communication instruments of the Department.

   b. Notify the officer in command of all irregularities of telephone or telephone instruments.

9. Radio test shall be given by the Bureau of Operational Control to ensure that the vocal alarm system and radios are properly functioning. These tests will be given at 0800 hours and at 1800 hours daily. Using the "Acknowledgement Lever" is required.

10. Activity sheets shall be prepared by the Bureau of Operational Control and shall cover the period from 0800 hours to 0800 hours of the following day. The information for the Activity Sheet shall be provided to the Bureau of Operational Control by the officer who is required to prepare the fire report after each response. The Activity Sheet prepared by the Bureau of Operational Control shall be forwarded to Headquarters immediately after 0800 hours.

11. Station Security:

   a. The on duty officer in command of each company in accordance with Department Regulations, is totally responsible for the security of the stations and equipment therein.

   b. Entry doors and windows shall be locked at all times. Keys shall be carried on apparatus. All entry doors and windows shall be checked to ensure that window locks, door locks and keys are functioning properly. When defects are found, notify Headquarters for corrections.

   c. All apparatus doors in fire stations shall be closed at all times except when responding to alarms or other appropriate reasons for apparatus to be taken from quarters. At that time, the doors shall be closed after leaving the stations.

   d. The doorbells on entry doors shall be checked periodically to ensure that they are functioning properly. As defects are found, notify Headquarters for correction.

   e. Members shall not permit children to enter quarters except when accompanied by parents or guardians.

   f. When visitors present themselves at quarters, members shall politely assertain their names and the nature of their business and notify the officer in command or the member concerned.

g. Members shall exclude from quarters all solicitors except those with official permission.

12. Outside visitors to fire stations are prohibited above the apparatus floor unless specifically authorized by the Chief of Department. Any outside visitor to any fire station shall be accompanied by the officer in command or an on duty member of the station. No visitor shall be allowed in the stations when the station is empty.

The General Order cancels and supersedes General Order #26-88 and replaces General Order #34-80.

By order of the Chief of Department,

Michael F. Moise
Chief of Department

APPROVED:

CHARLES A. PISATURO
COMMISSIONER OF PUBLIC SAFETY

9-19-88