The Human Factor in

COMPUTER CRIME

JULIA VAN DUYN

THE HUMAN FACTOR IN COMPUTER CRIME

J. Van Duyn

PETROCELLI BOOKS
Princeton, New Jersey

Designed by Diane L. Backes
Typesetting by Backes Graphics

Printed in the United States of America
First printing

Library of Congress Cataloging in Publication Data

Van Duyn, J.A., 1926-
The human factor in computer crime.

Bibliography: p.
Includes index.
1. Computer crimes—United States. 2. Electronic data processing departments—Security measures.
I. Title.
HV6773.2.V36 1984 364.1'68 84-20620
ISBN 0-89433-256-2

ACKNOWLEDGEMENTS

Among the many people who have helped shape this book and to whom I'm most grateful, I want to convey a special thanks to Dr. Ned Chapin for his incisive review and constructive suggestions. In addition, I wish to express my appreciation to the following individuals for their valuable help and cooperation:

Dean B. Allison Assistant United States
Attorney Chief, Major Frauds Unit
Los Angeles, California

Joe A. Nunez
Assistant Supervisor
Records & Exhibit Section
Los Angeles, California

Robert E. Killion, CSR
Official Court Reporter
Los Angeles, California

J. Van Duyn

Contents

1

Introduction

ONE
Introduction

To appreciate the extent to which human factor plays a part in computer crime, we have to be aware of its role in crime deterrence, prevention, detection, and risk assessment on the physical, hardware, software, and personnel security levels.

Considering the rather recent appreciation of the last security category, perhaps it isn't odd that at most DP facilities while great attention is afforded to physical, hardware, and software security measures and controls, little or no thought is given to personnel security. Yet, without effective personnel security, meaning a security program which is designed to foster the most effective deterrent against computer crime: *job satisfaction,* the most sophisticated hardware and software security systems are worthless.

This does not mean to imply that the first three computer security categories are not important insofar as computer crime countermeasures are concerned. Far from it.

Nevertheless, unless the human factor—an element often ignored by management and neglected by high technology technicians—is considered in every aspect of computer se-

curity, the business or government organization and its DP operations are highly vulnerable to computer crime, as the case histories offered in this book indicate.

The examples presented here also help to separate the myth and the recent nationwide hype about outsiders being the greatest threat to business and government DP security. The truth is that insiders pose a far greater threat to the organization's computer security than outside "electronic invaders" possibly could. The reason is pure and simple. Insiders are familiar with their employer's DP operations and the type of data each system and application is storing and processing. Consequently, they know where to look for specific data. And if they are in doubt, they can reference the systems' documentation which usually includes programming specifications, file and record layouts, a data element dictionary, and so on. But most significantly, insiders have or can somehow get the password to access stored crucial information such as financial, marketing, manufacturing, technological, or research data *unless* proper prevention and detection measures are in effect.

Before going any further, perhaps a definition of computer security is appropriate. Computer security, according to computer crime experts, is an umbrella that protects the organization's hardware and software, as well as the data and information processed by the computer against abuse, fraud, embezzlement, sabotage, and intentional or accidental damage, or natural disaster.

And who has the awesome responsibility to ensure that effective measures are installed and maintained? In the final analysis the security of the organization's computer equipment—the raw and processed data and information, *and* the personnel using these valuable resources—is the responsibility of top management.

Moreover, because computer security is a *management issue,* management must define and enunciate its *security philosophy* BEFORE setting up a computer security system, and perhaps even BEFORE a risk assessment is performed.

In balancing risk assessment with the level of risk the company can accept and the cost of computer security, the following legislative and regulatory requirements should be considered by management:

1.1 THE FOREIGN CORRUPT PRACTICES ACT OF 1977

Because by now all accounting and record keeping functions in both commercial and government organizations are performed by computers, the statute that has most impact on data processing security measures and controls is the Foreign Corrupt Practices Act of 1977—an amendment to the Securities and Exchange Act of 1934. The following presents pertinent parts of this significant law:

To begin with, its title is a misnomer. Its two main sections, *Accounting Standards* and *Foreign Corrupt Practices by Issuers,* affect *all* domestic and especially domestic public companies, as well as international corporations *that are subject to the Securities Exchange Act of 1934.* Specifically, through one of the Act's sections, entitled, *"Foreign Corrupt Practices by Domestic Concerns,"* the statute states that it applies to (a) any individual who is a citizen, national or resident of the U.S., (b) any corporation, partnership, association, joint-stock company, business, trust, unincorporated organization or sole proprietorship that has its principal place of business in the United States, or that is organized under the laws of a state, territory, possession or commonwealth of the United States.

Further, the *Accounting Standards* provision of the Act mandates that any company subject to the Securities Exchange Act of 1934 shall:

> "(A) make and keep books, records, and accounts, which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the company; and
>
> "(B) devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that—
>
> "(i) transactions are executed in accordance with management's general or specific authorization;
>
> "(ii) transactions are recorded as necessary (I) to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements, and (II) to maintain accountability for assets;
>
> "(iii) access to assets is permitted only in accordance with management's general or specific authorization; and
>
> "(iv) the recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences."

Noncompliance of this Act can effect fines and jail sentences for offending directors and officers.

A hindsight note relating to a case in point: If the above Act had been enacted eight years earlier, perhaps it would have served as a deterrence for Stanley Goldblum, the youthful Chairman of the Board of Equity Funding Life Insurance Company (EFLIC), and his two close associates from perpetrating the $200 million computer-related fraud that was in operation from 1969 until March 30, 1973.

Human factor, in the form of a disgruntled ex-employee, Ronald Secrist (at one time an EFLIC Assistant Vice President), initiated the first crack in the highly polished com-

puter-related scam. It seems that on March 7, 1973, Secrist, returning to the East Coast, contacted the Deputy Superintendent of the New York Insurance Department, who then telephoned Gleeson L. Payne, Insurance Commissioner of the State of California, about the top management of EFLIC being involved in writing and issuing large quantities of bogus policies.

The allegations were so "disturbing" that an investigation of EFLIC, which Payne earlier characterized as "one of the most efficiently run companies I know," and which was the "hottest stock" on the New York Stock Exchange began.

The genesis of Goldblum's computer-related fraud evolved from an interesting and, for a short time, highly successful idea: the Equity Funding Program. The concept, structured along the lines of the British Life Funding program and embellished by Goldblum, offered a highly salable and attractive combination of mutual funds and life insurance. Prospective customers were sold on the idea that by buying mutual fund shares, they could use the shares as collateral to purchase life insurance. Customers were assured that the dividends and appreciation of the mutual fund shares would pay for the insurance premiums and the interest on the borrowed amount.

However, the sales didn't come up to the expectation of the ambitious, enterprising, and highly sales-oriented Goldblum. To get a high volume of positive cashflow and an increased sales figure—both of which the company needed badly—Goldblum and his two associates came up with a "bold and creative" plan: issue fictitious life insurance policies for nonexisting people.

In carrying out the plan, records of the bogus policies were set up on the EFLIC computer as a subsystem, entitled "Department 99." This subsystem was partitioned

from the company's other systems, and accessible via a complex password only to top management and the programmer, specially chosen for the job to design, develop, and maintain the "highly confidential system."

Actually, EFLIC used computer hardware and software to an extent that was rather uncommon if not unique in commercial enterprises in 1969. The company had the general ledger, journals, accounts receivable/accounts payable, payroll, inventory, "in-force" policies, sales commissions, and all other business transactions processed and stored by the computer.

The EFLIC triumvirate's theoretical concept became a high-production reality, and a large quantity of bogus policies were issued and then sold to reinsurers, i.e., other life insurance companies. Selling policies to reinsurers in order to spread actuarial risks and obtain cash is a normal practice in the insurance industry. Thus, EFLIC received 180 percent, the usual insurance commission, on nonexistent premiums. And because the policies were counterfeit, the company didn't have to pay out any sales commission or any other of the many expenses connected with issuing legitimate life insurance policies. In short, the money that EFLIC got from reinsurers for the bogus policies was clear profit.

But it was a short range windfall because of the life insurance industry's regulations. These regulations mandate that the company originating the policies has to turn 90 percent of the first year premiums from the policyholders over to the reinsurer. Thus, after a year of issuing bogus policies, EFLIC had to pay out cash for the fictitious policyholders. This, in turn, forced the cash-tight EFLIC, that is Goldblum et al, to generate more and more counterfeit insurance policies to be sold to reinsurers.

There was still another *creative* way EFLIC management generated cashflow: They took an appropriate number of

fictious policyholders and simply put an end to their "computerized existence." The conspirators then filed with the reinsurers for death-benefit claims, labeling the sums they received as *current earnings* in the company's accounts.

In the meantime, the California Insurance Department and the Illinois Insurance Department (EFLIC, though headquartered in Studio City, California, was incorporated in Illinois) continued their examination of EFLIC's way of doing business.

As soon as word got out that examiners from two states were doing an in-depth audit of Equity Funding, stories of illegal opeations at EFLIC flooded Wall Street. The effect was predictable: Equity stock took a sharp decline on the New York Stock Exchange.

To counteract the rumors, Goldblum and one of his close associates flew to New York on Thursday, March 22, 1973. Goldblum gave several presentations to financial groups. He insisted that the states' auditing of his corporation's records was "a routine examination" and nothing more.

Notwithstanding all these last minute efforts, the order for seizure of the EFLIC company was served by the California Insurance Company at 6:30 PM Friday, March 30, 1973.

In April 1975, after the corporation went into bankruptcy under Chapter X, the forty-six year old Stanley Goldblum was sentenced to eight years at McNeil Island Federal Penitentiary, Washington. In addition, he was fined $20,000. While his two associates received seven years and five years respectively at different Federal Penitentiaries.

The Equity Funding caper, though it may not be "THE computer crime that started it all," as many computer experts claim, it certainly is one of the first computer-related frauds that gained national attention.

1.2 THE PRIVACY ACT OF 1974

Next in importance, insofar as management is concerned, is the Privacy Act of 1974. *Privacy,* as it relates to a collection of personal data, is very much a part of computer security. The Act involves the right of individuals to control or influence what information about them may be collected and stored, by whom, for what specific reasons, and to whom that information may then be disclosed.

The Privacy Act also covers the right of the individuals to know if information about them has been compiled, and if the said information is correct and complete. Furthermore, individuals have the right to challenge the accuracy of that information.

Technically, the Act is limited to government agencies and companies that work for them under contracts. However, the Act contains several provisions that are pertinent to computer security and possible computer crime at any DP facility.

For instance, the Act requires:

a. That each agency takes certain steps to maintain the security and confidentiality of records, and protects against any anticipated threats to security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

b. That each agency accurately record disclosures of certain types of information under that agency's control.

c. That each agency establish "rules of conduct" for persons involved in the design, development, operation, or maintenance of any system or records involving personal data.