Executive Summary

Computer systems are coming of age. As computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor system design, accidents that disable systems, and attacks on computer systems. Without more responsible design and use, system disruptions will increase, with harmful consequences for society. They will also result in lost opportunities from the failure to put computer and communications systems to their best use.

Many factors support this assessment, including the proliferation of computer systems into ever more applications, especially applications involving networking; the changing nature of the technology base; the increase in computer system expertise within the population, which increases the potential for system abuse; the increasingly global environment for business and research; and the global reach and interconnection of computer networks, which multiply system vulnerabilities. Also relevant are new efforts in Europe to promote and even mandate more trustworthy computer systems; European countries are strengthening their involvement in this arena, while the United States seems caught in a policy quagmire. Although recent and highly publicized abuses of computer systems may seem exceptional today, each illustrates potential problems that may be undetected and that are expected to become more common and even more disruptive. The nature and the magnitude of computer system problems are changing dramatically.

The nation is on the threshold of achieving a powerful information infrastructure that promises many benefits. But without adequate safeguards, we risk intrusions into personal privacy (given the growing electronic storage of personal information) and potential disasters that can cause economic and even human losses. For example, new vulnerabilities are emerging as computers become more common as components of medical and transportation equipment or more interconnected as components of domestic and international financial systems. Many disasters may result from intentional attacks on systems, which can be prevented, detected, or recovered from through better security. *The nation needs computer technology that supports substantially increased safety, reliability, and, in particular, security.*

Security refers to protection against unwanted disclosure, modification, or destruction of data in a system and also to the safeguarding of systems themselves. Security, safety, and reliability together are elements of system trustworthiness—which inspires the confidence that a system will do what it is expected to do.

In many ways the problem of making computer and communications systems more secure is a technical problem. Unlike a file cabinet, a computer system can help to protect itself; there exists technology to build a variety of safeguards into computer systems. As a result, software, hardware, and system development presents opportunities for increasing security. Yet known techniques are not being used, and development of better techniques is lagging in the United States. From a technical perspective, making computer system technology more secure and trustworthy involves assessing what is at risk, articulating objectives and requirements for systems, researching and developing technology to satisfy system requirements, and providing for independent evaluation of the key features (to assess functionality) and their strength (to provide assurance). All of these activities interact.

Attaining increased security, in addition to being a technical matter is also a management and social problem: what is built and sold depends on how systems are designed, purchased, and used. In today's market, demand for trustworthy systems is limited and is concentrated in the defense community and industries, such as banking, that have very high levels of need for security. That today's commercial systems provide only limited safeguards reflects limited awareness among developers, managers, and the general population of the threats, vulnerabilities, and possible safeguards. Most consumers have no real-world understanding of these concepts and cannot choose products wisely or make sound decisions about how to use them. Practical security specialists and professional societies have emerged and have begun to affect security practice from inside organizations, but their impact is constrained by lack of both management

1

Overview and Recommendations

We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb.

To date, we have been remarkably lucky. Yes, there has been theft of money and information, although how much has been stolen is impossible to know.[1] Yes, lives have been lost because of computer errors. Yes, computer failures have disrupted communication and financial systems. But, as far as we can tell, there has been no successful systematic attempt to subvert any of our critical computing systems. Unfortunately, there is reason to believe that our luck will soon run out. Thus far we have relied on the absence of malicious people who are both capable and motivated. We can no longer do so. We must instead attempt to build computer systems that are secure and trustworthy.

In this report, the committee considers the degree to which a computer system and the information it holds can be protected and preserved. This requirement, which is referred to here as computer security, is a broad concept; security can be compromised by bad system design, imperfect implementation, weak administration of procedures, or through accidents, which can facilitate attacks. Of course, if we are to trust our systems, they must survive accidents as well as attack. Security supports overall trustworthiness, and vice versa.

COMPUTER SYSTEM SECURITY CONCERNS

Security is a concern of organizations with assets that are controlled by computer systems. By accessing or altering data, an attacker can steal tangible assets or lead an organization to take actions it would not otherwise take. By merely examining data, an attacker can gain a competitive advantage, without the owner of the data being any the wiser.

Computer security is also a concern of individuals, including many who neither use nor possess computer systems (Box 1.1). If data can be accessed improperly, or if systems lack adequate safeguards, harm may come not only to the owner of the data, but also to those to whom the data refers. The volume and nature of computerized data-bases mean that most of us run the risk of having our privacy violated in serious ways. This is particularly worrisome, since those in a position to protect our privacy may have little incentive to do so (Turn, 1990).

The threats to U.S. computer systems are international, and sometimes also political. The international nature of military and intelligence threats has always been recognized and addressed by the U.S. government. But a broader international threat to U.S. information resources is emerging with the proliferation of international computer networking—involving systems for researchers, companies, and other organizations and individuals—and a shift from conventional military conflict to economic competition.[2] The concentration of information and economic activity in computer systems makes those systems an attractive target to hostile entities. This prospect raises questions about the intersection of economic and national security interests and the design of appropriate security strategies for the public and private sectors. Finally, politically motivated attacks may also target a new class of system that is neither commercial nor military: computerized voting systems.[3]

Outside of the government, attention to computer and communications security has been episodic and fragmented. It has grown by spurts in response to highly publicized events, such as the politically motivated attacks on computer centers in the 1960s and 1970s and the more recent rash of computer viruses and penetrations of networked computer systems.[4] Commercial organizations have typically concentrated on abuses by individuals authorized to use their systems, which typically have a security level that prevents only the most straightforward of attacks.