1.10 Law and Network Security

An increasing number of legal issues affect how administrators approach network security. If your organisation is a publicly traded company, a government agency, or does business with either, there may be legal constraints before choosing your security approach. Legal constraints include any laws that affect how information is stored or accessed. Even if your network is not legally bound to these security guidelines, reviewing the various laws that impact your computer's security is extremely useful.

One of the oldest pieces of legislation in the United States affecting computer security is the Computer Security Act of 1987 (100th Congress, 1987). This act requires government agencies to identify sensitive systems, conduct computer security training, and develop computer security plans. This law is a vague mandate ordering federal agencies in the United States to establish security measures without specifying any standards.

This legislation established a legal mandate to enact specific standards, paving the way for future guidelines and regulations. It also helped define certain terms, such as what information is indeed "sensitive," according to the following quote found in the legislation itself:

Sensitive information is any information, the loss, misuse, or unauthorised access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorised under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defence or foreign policy.

Keep this definition in mind as it is not just Social Security information or medical history that must be secured. When considering what information needs to be secure, simply ask the question: Would the unauthorised access or modification of this information adversely affect my organisation? If the answer is "yes," then you must consider that information "sensitive" and implicate certain security precautions.

The Computer Misuse Act 1990 is the base law for all other computer related laws in the UK. It applies for the whole of the UK and is usually the underlying law used to charge a suspect over a computer crime. Crimes like credential stealing, hacking and phishing. These are considered Section 1 offences, which can lead to 6 months to 2 years in prison. Section 2 crimes are the crimes intended to be performed, after a hacker has penetrated the system, such as using the credentials stolen to access a server, or committing fraud. Being found guilty under the section 2 act of the computer misuse act can lead to up to 5 years in prison.

Keep in mind that any law which governs privacy (such as the Health Insurance Portability and Accountability Act [HIPAA], for medical records) also has a direct impact on computer security. If a system is compromised and its data is covered under any compromised privacy statute, you might need to prove that you exercised due diligence to protect that data. If you fail to take proper precautions, it could result in civil liability.