Introduction

Securing electronic commerce has become an increasing issue as new applications and internet based infrastructures are manufactured. As new technologies are on the rise so are security exploits in relation. A simple violation could be just a mailing address being discovered or larger than the breaching of a network with thousands of clients’ sensitive information. All electronic data you send, read, and receive involve a risk. When the dependency on technology raises so does the volume of risk. Causing the strain for all-inclusive security programs and network security jobs more difficult.

New Internet security exposures revealed almost daily. These findings can be credited to failings in software or the result of software configuration errors. These weaknesses can be exploited by hackers and malicious persons to gain entree to the system.

The confidentiality, integrity, and availability of information on the Internet are three basic security concepts [8]. Information that is read or copied by someone not authorized to do so is known as loss of confidentiality. Information that has been classified as confidential is usually private or sensitive and should not be disclosed. Examples of this type of information include credit card applications, medical records, bank records, and corporate business plans. If information is available on an insecure network it can be corrupted. The result is a loss of integrity because the information has been modified in an unexpected way. Unauthorized changes have been made to the information, sometimes by human error or intentional tampering. Integrity of information is important for activities such as electronic funds transfers and air traffic control. The loss of availability is when information is erased or becomes inaccessible. This means that people who are authorized to get information cannot get what they need. Availability is important to service-oriented businesses that depend on information. Availability of the network itself is important to anyone whose business or education relies on a network connection (Gehling and Stankard 32).

Research on securing electronic commerce is extensive. Electronic data interchange and secure online transactions are key perceptions to focus on to improve security. Through Computing/Technology Policy, commerce policy and computer crime are major components to understand. Lastly, security services and Software and Application Security are vital areas maintain when securing electronic commerce.