CHAPTER 1

Introduction to Security

Scenario 1: A post on http://threatpost.com, Threatpost, the Kaspersky Lab Security News Service, dated August 5th, 2013 with the title "BREACH Compression Attack Steals HTTPS Secrets in Under 30 Seconds" by Michael Mimoso, states[1]:

> "A serious attack against ciphertext secrets, buried inside HTTPS responses, has prompted an advisory from Homeland Security.
>
> The BREACH attack is an offshoot of CRIME, which was thought dead and buried after it was disclosed in September. Released at last week's Black Hat USA 2013, BREACH enables an attacker to read encrypted messages over the Web by injecting plaintext into an HTTPS request, and measuring compression changes.
>
> Researchers Angelo Prado, Neal Harris, and Yoel Gluck demonstrated the attack against Outlook Web Access (OWA) at Black Hat. Once the Web application was opened and the Breach attack was launched, within 30 seconds, the attackers had extracted the secret."

Scenario 2: A post on http://threatpost.com, Threatpost, the Kaspersky Lab Security News Service, dated December 30th, 2013 with the title: "Most Surprising NSA Capability: Defeating the Collective Security Prowess of the Silicon Valley" by Dennis Fisher, states as follows[2]:

> "Some of the earliest leaks to emerge from the Edward Snowden cache described a program called PRISM that granted the NSA "direct access" to networks run by Google, Yahoo, Microsoft, and many other companies. That direct access was quickly interpreted to mean that those companies were giving the agency data links to their servers through which the NSA could collect traffic information on targets. The affected companies quickly denied this; only later was it revealed that "direct access" came in the form of tapping undersea cables that carry unencrypted traffic between data centers around the world. The revelation triggered an immediate response from Google, Microsoft, and Yahoo, who said that they would be encrypting that traffic in the near future. In addition, some Google engineers had some choice words for the NSA's in-house hackers. In the words of Google's Mike Hearn, "The traffic shown in the slides below is now all encrypted and the work the NSA/GCHQ staff did on understanding it is ruined."

What is Security?

The events above are a few of the security breaches that were reported during 2013. There are many security breaches reported every year from different quarters of the world. Some of these may be accidental and some intentional. Some may not be with the intention of making money, while others are done purely with the intention of making money. Some events may be done for one-upmanship or merely for the thrill of breaking the system. With more computers and people interconnected and in turn, connected by the internet, the role of computer security in general and

information security in particular, with special emphasis on cybersecurity, is gaining momentum. With technological advances and the spread of technological know-how, information security is certainly a humongous task for everyone! That is, all computer users including the non-technical ones.

Our intention here is not to define the term "security," but to explore the term so that it becomes crystal clear to the readers as to what it really means. A basic animal instinct is to ensure one's own "safety." Every animal, including a human, will fight for its safety. Everyone wants to be safe and preserve whatever they have with them whether that be assets, money, or otherwise. The security of the individual, company, assets, or security of their information and many more similar things are expected and seem to be quite in sync with nature's laws. Security, in simple terms, is protecting what you or others have. This same idea applies to entities like government departments, agencies, companies, institutes, and so on, irrespective of their size or function.

The security of not only physical assets, but of non-physical assets as well are important and necessary. Some of these non-physical assets include confidential information and data; intellectual property; research data with the potential of high value realization and high investment; and the security of your customers or end users when at your facility or while using your systems. The security of the installations with high defense or strategic value, like nuclear installations, nuclear sources, chemical and biological laboratories, and areas with high-level political and administrative dignitaries, are of significance. Most terrorist threats are guided (or misguided) by so-called ideals or ulterior motives, making the security more important. Security is even more important with the recent rise in widespread use of technology such as mobile phones, the internet, tablets, and other mobile devices. Disgruntled or unhappy employees are also achieving significance by leaking information that is of strategic importance, either for exacting vengeance or for profit.

Why is Security Important?

Earning is difficult, but losing is extremely easy. You have to earn with your efforts, but you can lose because of others' efforts. No individual or entity wants to lose what they have earned through hard work (or even otherwise!). If you lose what you have, you have to start over again, which is hard for anyone. Again, by nature, everyone wants to preserve their energy and secure their future for themselves and their children. Every organization wants to secure its bright future. Securing what you have and not losing it, while getting more of it, is important for societal status. Every individual or organization is a "social animal" and is conscious about their status. Status is what makes one distinct or different from others. Organizations or governments have a lot of information at their fingertips which is of strategic importance to them. They invest a lot in carrying out research in areas of strategic, military, or competitive significance to them. The loss of this information to a third party with the same interests may lead to their strategy being a complete waste, thereby leading to the waste of entire investments and years of effort. This may require them to restart their efforts, possibly using a new way of thinking. Information may be required by those who want it for the value of it, or who want to show their heroism. Some of the current generation of so-called computer hackers may just want to satisfy their ego or show their supremacy over the technology and may steal useful and valuable information and publish it to others. Others may want to mine for data of value so that they can sell the same to others, who want the information to either harm others or make commercial gains from it. Terrorists may want the information to either destroy the strategic or military capability of a country, or to threaten the economy of a country by using the information they steal. Also, 3D printers present a new possible threat by potentially being used by terrorists to create weapons! The primary reason for information security is the threat of information being misused if it lands in the wrong hands.

Some people feel that the need for information security is "hyped." However, we in technology security do not think so. It is possible to think of information security as "hyped" only if our focus is on information security just for the sake of information security, and not based on the risks to the business of any information leakage, breakage, or loss. The protection of business information of value is the primary reason for information security. We must ask ourselves, "Can we risk the leakage of customer data held by us or to which we have access?" If the answer is "no," then we have used basic Risk Management to justify a need for security because the leakage of customer data can only be at our own peril.

Furthermore, the pace at which we are coming up with new technologies is also of concern to security. New technology, new products, and new applications are brought to the market with such speed that inherent security issues may not be known yet and it may not have been possible to be tested thoroughly before launch. Once new

technologies are in the market, there is a possibility that somebody may accidentally or intentionally break through any of the inherent security flaws in the technology, product, or application. It is necessary that entities or individuals have the capability to be able to respond at such a speed that the chances of an exploitation of a security flaw are very minimal. Many times, it may not be possible to do so because of design or technical issues behind the flaw, or because of the extent to which the solution is required, sometimes across multiple systems and by multiple users. This means that some of the entities or users are open to the exploitation of such a security flaw. Oftentimes, users and entities may not apply the corrective actions immediately, either because of a lack of appreciation of the gravity of the issue, because of ignorance, or because of other priorities. This is very much true when there are deadlines to be met and many of the compulsory checks get skipped due to lack of time or personnel to perform those checks.

Science and technology provide many tools which are at the disposal of entities and people that can be used for either good purposes or bad purposes. Bad guys can always use such facilities or tools for bad purposes. For example, a security tool like Metasploit or Nessus or nMap, if placed in an auditor's hands, can harden infrastructure, whereas in a cracker's hands they become the go-to tools for criminal activity. A proper focus on information security allows only the required details about the entity or person to be known to the outside world. If any entity or person wants "peace of mind" in today's connected world, information security is a MUST.

■ **Note** Sometimes the book might appear to use the terms "cracker" and "hacker" interchangeably. However, they are different. A cracker is the name given to a hacker who breaks into computers for criminal gain. A hacker, however, can also be an internet security expert who is hired to find vulnerabilities in systems.

What if You Do Not Care About Security?

If you think you don't need to care about information security, you are creating more risk than you bargained for. With advanced technologies at the disposal of many people, it is only a matter of time until you are robbed or your reputation is tarnished. Hence, at this time, no person or entity can ignore or take its own security lightly, making it hard to sleep at night! For example, you could find that if you doze off, and ten minutes have passed, your debit card could be stolen by someone and already, all the money in your account could be swindled by someone. Maybe your laptop is stolen and the new proposal of millions of dollars you have been working on quite painstakingly is already in the hands of your competitors. Maybe the innovative concept you have been discussing over the phone is overheard, recorded, and patented by someone else. There are unlimited possibilities as to what can go wrong. If you do not care about security, your existence itself will be at risk. Beware of this!

There are instances of Automated Teller Machines (ATMs) being towed away or otherwise hacked by thieves. There are many instances where information has been stolen from emails, laptops, or cell phones and used to blackmail the owners.

There have been instances of weak encryption being substituted by strong encryption, and entities/people have been blackmailed have had to shell out significant amounts of money to get the data decrypted. There have been instances where passwords have been changed or servers have been overtaken by others and then thieves demand a ransom to restore access. There have been instances where software applications have been pirated by overcoming built-in controls and thus, the entity that created the software loses a significant amount of revenue.

There have also been instances of identity theft, which can lead to huge losses. There have been instances where the data of strategic and military importance has been stolen physically or through logical means of hacking. There have been instances of gaining physical entry into secure areas and destroying crucial assets, including information assets. There have been instances where the data has been compromised, either by luring the people or by other means, which leads the party to huge losses. We cannot even fully imagine the kind of possibilities that are out there. Perhaps, the hacker is even able to intervene with the navigation system of an airplane or a missile and bring it down or make it strike somewhere else! The possibilities are endless, and we do not know the extent of damage information in the wrong hands could potentially cause. We can continue citing examples, but we hope to bring as many instances as possible to your attention as we write this book.

We have seen or heard of instances of hacking into banking accounts and initiating transactions or hacking into systems and obtaining credit card or debit card related information or credentials such as PIN or Telephonic PIN and misusing them. Phishing attacks are common as are instances of credit cards or debit cards being cloned. There have been instances of identity theft and fake profiles created on social media. Social engineering attacks, where attackers befriend persons and later misuse the information or relationship obtained, are becoming common.

Malicious software attacks through links or attachments in emails, through add-ins to the browser, or through the download of free applications or games is common. Tracking or hacking through mobile devices is a recent phenomenon that must be monitored. Exploiting the technical vulnerabilities of the applications, protocols, web browsers, web servers, or utilities is also a known phenomenon.

Eavesdropping on wireless communications or misusing wireless connections is on the rise. The rogue wireless access points set up by attackers attract many users which leads to the compromise of important information like login credentials.

In addition to the above, ineffective maintenance of the systems or utilities such as UPS or electrical cables can lead to system failure, thus reducing productivity.

There have also been instances of misuse of surveillance cameras, remote connection utilities used to hack into someone else's system, and application errors not known or not fixed by the vendor organizations.

With a lot of information getting distributed easily across the globe because of Web and Cloud technologies, there are a lot of challenges to ensure that data and information of value are well protected so that they are not compromised.

The Evolution of the Computer and Information Security

If you glance through the history of computer security, you will find that the initial need was to physically protect the mainframe computers, which were used to crack the encrypted messages used during the world wars. Physical security was provided through security guards, identification cards, badges, keys, and other means. These regulated the access to sites and locations where the mainframe computers were hosted and were essential for protecting them from theft and destruction. This was the main scenario during the 1950s and 1960s.

ARPAnet, the precursor to the Internet, was started with the intent of sharing data between remote locations. With the primary intention of ARPAnet being a provision of connectivity across various locations and systems, information security does not seem to have been given much importance. However, as the days progressed and more data and more people came on to ARPAnet, linking many computers, the need for information security increased.[5]

The MULTICS, multi-users, and timesharing operating systems increased the need for information security. MULTICS (Multiplexed Information and Computing Services) operating system, true to its name, facilitated many different users to access the system simultaneously. The MULTICS was a research project started at MIT in 1964 and sponsored by Honeywell, GE, and MIT that allowed multi-user capability serving thousands in academic and research communities. This operating system provided much-needed focus on computer security and was built into the requirements for computer security. Honeywell then dropped out of the consortium to develop its own product. MULTICS systems were eventually sold for commercial use by Honeywell, with both the security and services.

Multi-user systems allow hardware and software applications to be accessed by multiple users. Multiple users can access the single system from the same location or a remote location using different computer terminals with different operating systems. These terminals are connected through wires and telephone networks. Since systems were shared by users who might not trust each other, security was of major concern and services were developed to support security features for file sharing via access control. MULTICS machines were developed to protect data from other users. Information co-existed on the same machine and the data was marked as 'Confidential,' 'Classified,' etc. Operating systems were designed to ensure that the right data is accessed by the right user.[6]

Ken Thomson from Bell Labs liked the MULTICS system but felt it was too complex and the same idea could be implemented in a simpler way. In 1969, he wrote the first version of Unix, called UNICS (Uniplexed Operating and Computing Systems). In 1973, Ken Thomson and Denise Ritchie wrote the first C compiler and rewrote Unix in C. The following year, Unix was licensed to various universities. University of California Berkley modified UNIX and called their version "BSD" Unix, and Bell Labs continued to use Unix under the name "System V-+" Unix. Eventually, there were two types of Unix operating systems: BSD and System V. The biggest advantage Unix had was its networking capabilities.

Unix became an ideal operating system for connecting different systems and providing e-mail services. It supported the TCP/IP protocol for computer communication. It also provided security features like user authentication mechanisms through user ID and password, different levels of access, and restrictions at the file level.[6]

In the mid 1970s, the invention of microprocessors led to a new age of computing with the introduction of Personal Computers (PCs). The 1980s gave rise to wider computer communication through the interconnection of personal computers, mainframe computers, and mini computers. This enabled resources to be available to all users within a networking community and led to the need for complex information security. As the popularity of PCs grew, networks of computers became more common as did the need to connect these computer systems together. This gave rise to the birth of the Internet. In the 1990s, the Internet was made available to the general public. The Internet virtually connected all computers over a pre-existing telephone infrastructure. After the Internet was commercialized, the technology became pervasive, connecting every corner of the globe. However, initial days of internetworking experienced many issues because of factors like incompatibility of the proprietary protocols not allowing proper communications between two systems/networks, different vendors using different technologies to ensure their stronghold on the technology, and difficulties in ensuring that the message intended reaches only the destination device. Routing technologies, standardization efforts on the protocols, and standardization of computer systems and logical addressing systems like IP changed the scenario over time and enabled easy communication between various devices on the internet.

Tim Berners Lee wrote the first web page and the first web server.[7] He designed the World Wide Web (WWW) to link and share news, documents, and data anywhere in the network. By 1991, people outside CERN joined the web community and in April 1993, World Wide Web technology was made available to the public. Since that time, the web has changed the world. It has become the most powerful communication medium today. More than 30% of people in the world today are connected to the web. The WWW has changed the way we communicate with people, the way we learn new things, the way we do business, the way we share information, and also the way we solve problems. It has allowed everyone to not only be connected to one another, but also enables the sharing of information widely across the globe.[8]

The growth of the web has been phenomenal. There are more people communicating online today than any other medium. More shoppers buy and sell online today than in any other retail store. The rapid growth of the web and web usage has brought about many innovative developments. The web has several layers of technologies that all work together to deliver communication to the user. Today, the Internet has connected millions of "unsecured" computers together. This has been enabled through the growth of networking technologies and equipment like switches, multi-layered switches, and routers coupled with standardization of various protocols used. The switches enable connecting many machines within an organization and ensuring the frames are passed on appropriately to the intended destination computer whereas routers play a large role in routing the messages/communications from one network to the other and also connect to the internet. Routers are intelligent equipment and route the messages/communications efficiently from the source to the destination and connect to the internet. Also, many of the routers are now built with firewall capabilities. Advanced routers may act as switches as well as router. DHCP, NAT, and DNS have made the configuration and routing easy.

The vulnerability of information on each computer depends on the level of security provided by each system and to the system to which it is connected. Recent cyber threats have made organizations and governments realize the importance of information security. Information security has now become one of the major technologies to support the smooth operation of the Word Wide Web and Internet.

With the invention of the World Wide Web and the Internet, millions of users are connected and communicating with each other. This has raised several concerns regarding the integrity of the user, confidentiality of data, types of data that are being shared in the system, who is accessing the data, who is monitoring the information that is being sent on the Internet, and many more concerns related to information security. With the advancement of technologies such as wireless and cellular, users are always connected and networked computing has become the prevailing style of computing. As information became more exposed to the outside world, securing information has become a major challenge in the era of Inter-networking.

Information security is meant to protect information and information systems from unauthorized users accessing, using, modifying, or destroying the information. According to the standards defined by the Committee on National Security Systems, information security is the protection of information and its critical elements, including systems and hardware that uses, stores, and transmits that information. Security is achieved by implementing

policies, guidelines, procedures, governance, and other software functions. Information security consists of three main components: hardware, software, and a communication system.

Various tools are developed daily to combat the compromise of information security. Several standards and guidelines have been implemented to reduce the propensity for information security breaches. However, in a constantly evolving world, information security will always be a matter of concern that will need to be addressed for the good of the world!

Information security also spans to physical aspects like hardware and infrastructure, the operating system, networks, applications, software systems, utilities, and tools. Other important contributors (favorable or adverse) to the field of information security are human beings, particularly employees, contractors, system providers, hackers, and crackers.

Information Security Today

Let's explore information security in today's context. Information security is a matter of concern for organizations and individuals alike. Modern hackers are equipped with technological knowledge and tools to infiltrate the accounts of individuals and their credit and debit cards.

Thieves and the authorities are constantly at odds. Most often, thieves are beating the authorities. Many times, the police learn a new technique only after thieves have used it. Similarly, in the field of information, there is always a race between hackers and crackers and the information security personnel. With widespread use of Information Technology and related tools, particularly with the advent of the Internet, it has become a challenge for organizations and their employees to prevent the misuse of information.

Information in lay terms is anything that is communicated in any form, public or private. Any compromise of private information to others can have a significant impact on the parties involved, including the loss of reputation, finances, or other consequences depending upon the nature of the information. All forms of technology, including the Internet, credit cards or debit cards, ATMs, bank web portals, and so on, are all under attack; most times intentionally, sometimes accidentally.

Cloud computing is the popular buzz word today and has many benefits but also presents many new risks. A contextual illustration of this scenario is given in Figure 1-1. The rise in the use of electronic chips in everything from automobiles to refrigerators to TVs is another cause for concern. Theories of such attacks are emerging every day. This possibility is illustrated in Figure 1-2.

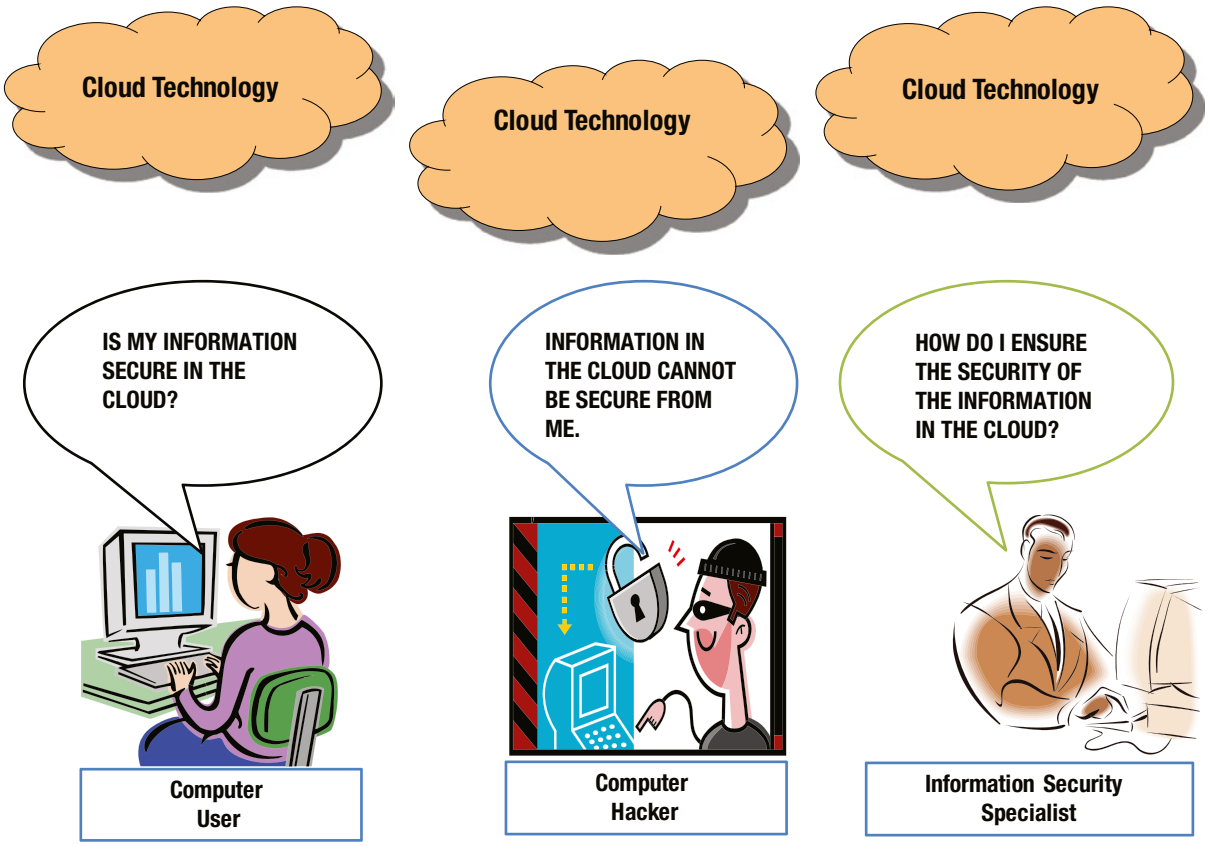

Figure 1-1. *Mistrust on "Cloud" and its security*

SCENARIO OF THE FUTURE?

Figure 1-2. *Is this the future state of security?*

Information security is an extension of computer security and extends beyond physical control to logical control, control over media, and control over a medium of communication. Information security should be one of the most important goals of everyone, including employees, contractors, suppliers/vendors, and other service providers. Even though there is growing recognition of this fact, there is still a lot more that needs to be understood and implemented by all the stakeholders involved.

In this fast-paced world, where information is an asset and the achievement of business objectives is everybody's responsibility, ensuring that the information security risks are minimized with the appropriate controls in place, has become a top priority. Of course, it is not always possible to eliminate all the vulnerabilities and consequential threats, but it is necessary to identify the risks to minimize the overall risk to the organization. It is also necessary that organizational management understands the residual risks created by the controls they have put in place. A proper and appropriate risk assessment and management methodology is one of the prime necessities of an information security framework.

As the old adage goes, "An ounce of prevention is worth a pound of cure." It is always better to put on our critical thinking caps and consider what can go wrong and have the appropriate solutions in place than to worry after an incident has taken place and cost us our reputation or significant monetary loss, either in terms of penalty or in terms of consequential damages.

Even with the utmost sincerity and tremendous efforts, it is not possible to have 100% foolproof information security, because while there may be many known issues, there may also be an equal number of hidden ones. However, if we do not make sincere efforts to at least contain known security flaws or security issues which are applicable to our organization, we do an injustice not only to ourselves and to our customers, but also to the world at large.

Customers have also started explicitly looking for information security being implemented whenever they purchase a system, software, or application. They will not be inclined to purchase any product with known security flaws. As such, product companies, as well as service companies, are required to focus more on information security. What better place to start information security than right at the requirements phase and carry it through during the design, development, testing, and deployment phases? Secure coding practices are gaining momentum and are going to be one of the focus areas of the future.

The following information sheds light on the current information security environment:

"The Norton Report[3] (for 2013), now in its fourth year, is an annual research study, commissioned by Symantec, which examines consumers' online behaviors, attitudes, security habits, and the dangers and financial cost of cybercrime." The Norton Report highlights the following information[3]:

- Consumers are more mobile than ever, but are leaving security behind. Despite the fact that 63% of those surveyed own smartphones and 30% own tablets, nearly one out of two users don't take basic precautions such as using passwords, having security software, or backing up files on their mobile device.
- Cybercrime continues to be a growing global concern. Both the total global direct cost of cybercrime (US $113 billion; up from $110 billion) and the average cost per victim of cybercrime ($298; up from $197) increased this year.
- As people are now constantly connected, the lines are blurring between their personal and work lives, across multiple devices and storage solutions. Nearly half (49%) of the respondents report using their personal devices (PCs, laptops, smartphones, tablets) for work-related activities."

Information security is often not given adequate attention primarily based on the false theory that the risk is low. It is also possible that many times, we try to use complex solutions rather than simple solutions. Whatever the method of implementation, information security has become imperative.

Applicable Standards and Certifications

In order to ensure information security, various efforts have been made by the industry in the form of standards and certifications. Some of the popular ones are ISO/IEC 27001:2005[4] (revised in 2013) — Information Systems Security Management System — Requirements by the International Organization for Standardization (based on ISO/IEC 27002), Payment Card Industry Data Security Standard (PCI DSS) by PCI Security Standards Council, Payment Application Data Security Standard (PA-DSS) by the PCI Security Standards Council, Control Objectives for IT and related Technology (COBIT) by Information Systems Audit and Control Association, ISO 20000-1:2011[4] i.e. Information technology — Service Management — Part 1: Service management system requirements. These are the standards against which an organization or an application can get certified (as appropriate) to or adapted by an organization to improve itself and provide a base for the compliance check for others.

Some of the other related regulations/framework of importance are: Sarbanes-Oxley Act of 2002 also known as SOX, Committee Of Sponsoring Organization of the Treadway Commission (COSO) framework, the Health Insurance Portability And Accountability Act (HIPAA) of 1996, Federal Information Security Management Act (FISMA) of 2002, Federal Information Processing Standards (FIPS) released by the National Institute of Standards and Technology (NIST), just to name a few.

Some of the other standards of relevance are: ISO/IEC 15408-1:2009 - Information technology — Security techniques — Evaluation criteria for IT security — Part 1: Introduction and general model[4]; ISO/IEC 15408-2:2008 - Information technology -- Security techniques — Evaluation criteria for IT security — Part 2: Security

functional components[4]; ISO/IEC 15408-3 - Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance components[4]; ISO/IEC 18405:2008 - Information technology — Security techniques — Methodology for IT security evaluation[4]. The International Organization for Standardization has also published many more guidelines for security professionals[4]. Furthermore, organizations like Information Systems Audit and Control Association in the U.S. have published many useful models and papers on information security.

We will elaborate on the above as it becomes relevant in subsequent chapters of this book.

The Role of a Security Program

Typically, a lack of awareness is one of the prime reasons for not adhering to requisite security guidelines and consequential security breaches. For instance, when a person ignores an advisory about how laptops left visibly in cars can be stolen or a travel advisory warning against travelling by taxi or other unknown vehicle, there is an increased risk for information security breach. Similarly, failure to create a strong password on your work computer can result in information security breaches at many levels, endangering you and your organization's reputation.

Awareness is the number one step in ensuring security, both physical security and information security. Awareness ensures that the chances or risks of vulnerability and threats to security are reduced considerably. Toward this end, it is essential to provide organizationwide security awareness programs to all employees (permanent or temporary), contractors, suppliers/vendors, customers, and all other relevant stakeholders who have access to the organization or its information. In order to achieve this, organizations need to ensure regular security awareness programs spanning various aspects of their life in the organization, clearly explaining what can go wrong. However, to ensure that all these stakeholders understand why security is important, it is essential for the success of any security program. Still, as the saying goes, "Knowing but not doing is equivalent to not knowing at all", and it is up to the individual participants of these programs to take the message and content of these programs seriously and implement them in letter and in spirit.

It is not enough that such a security program is in place and is conducted only once for the entire organization. This has to be an ongoing process to ensure that any new stakeholders, including new employees, are trained invariably. In addition, the organizational structure and environment (internal and/or external) may undergo changes which may lead to different vulnerabilities and threats. Hence, it is necessary that these programs are regularly reviewed, updated, and all the relevant stakeholders are trained on the changed scenarios and made aware of new risks.

All programs should take into account the risks the organization is currently undertaking and the controls they have painstakingly put in place for any security violation which defeats the very purpose of such controls. Involving each and every person is important for the success of any Security Program. Any person who is not aware of the security requirements, like a new security guard, employee, system administrator, or a new manager, can endanger the entire organization.

Moreover, in addition to the regular security programs as mentioned above, strong audits/assessments/compliance checks to ensure compliance to the policies, processes, and instructions of the company towards its security are to be adhered to without fail. A good execution is required to ensure the success of any well-intended program. However, execution is possibly the weakest link when it comes to most of the entities as well as most countries. Hence, regular checks carried out by competent and independent personnel of the organization or external agencies who do it not for the sake of just checking, but carry them out with the true intention and goal of bringing out any compliance weaknesses to the fore, is essential. Many times, reports of such compliance checks are beautifully made and wonderfully presented to the management but more often are totally forgotten, which could eventually lead to these documents creating liabilities when the suggested resolutions are not acted upon. Any compliance check with actions not being taken seriously on weaknesses found during the check is as good as a compliance check not being carried out in the first place! The better the compliance check carried out with extreme focus by the competent personnel and with extreme focus on the actions to be taken (and actually taken), the better the entity will be!