Journal of Higher Education and Learning
ISSN 2998-7679
Vol. 3, No. 1, 2026
Published by STSL Press

Original Paper

A Top-Down Approach to Providing Information Security Education to Non-STEM Students

Suchinthi Fernando[1]

[1] School of Communication & Information, Rutgers University, New Brunswick, NJ, USA

Correspondence: Suchinthi Fernando, School of Communication & Information, Rutgers University, New Brunswick, NJ, USA. E-mail address: suchinthi.fernando@rutgers.edu

Abstract

This paper discusses how at least a basic education in information security is required by everybody. Today's explosion of information – where misinformation and disinformation are abundant, and generative artificial intelligence (AI) makes distinguishing true facts from falsely created information difficult – requires anyone using, accessing, or sharing information to obtain at least a basic education in information security. Being a subject area in the science, technology, engineering, and mathematics (STEM) category, a thorough education in information security requires a strong mathematical background. This should not prevent the majority of information users, from non-STEM backgrounds, from obtaining a basic level of information security education. While students pursuing careers in information and cybersecurity require a deeper level of education, founded on a strong STEM background, the others, who require only a basic education in information security, so that they may access and share their information securely, may obtain it without a STEM background, by studying only the mandatory STEM concepts behind information security. As the usual bottom-up approach of first providing the mathematical foundation and then building the information security education atop that could overwhelm non-STEM students, instead, this paper proposes a top-down approach for providing basic information security education to non-STEM students. By teaching the mandatory STEM concepts behind information security in a natural manner stemming from day-to-day occurrences rather than deriving them through mathematical laws and processes, this approach allows non-STEM students to successfully obtain the basic information security education they require.

Keywords: information security, education, non-STEM students, STEM, top-down approach

1. Introduction

Every person uses, accesses, gathers, and shares information in some way, for their jobs, as well as for their personal lives. Accurate and up-to-date information is required to make informed decisions and take calculated risks, and information management and usage entails not only gaining access to accurate information, but also maintaining its integrity, and preserving its confidentiality to ensure the privacy of those involved (Fernando, 2018). Information security is acknowledged as a journey and not simply as an end destination, and is incorporated at all levels in a business by setting up the required perimeter, hardware and software security systems in place and laying out information security policies and procedures. Yet, the weakest link in all these security systems remains to be the users of information systems. Regardless of the strength of the technological security measures and policies, procedures, and protocols, if these are not properly administered or followed, then a system remains vulnerable (Fernando, 2018). Information systems – either digital, or otherwise – make the access and sharing of information efficient, enabling proper and secure access to information and allowing the sharing or communication of information with authorized users through authorized channels instead of simply allowing access to anyone. Therefore, in order to properly use these information systems, and access and share information in a secure manner, while ensuring their privacy, as well as the confidentiality and integrity of the information, one requires at least a basic understanding of information security. Especially in today's world where there is an explosion of information, and an abundance of misinformation and disinformation, and where generative AI is sometimes used to create false information, making it difficult to properly distinguish the true facts from the false, and where there is a multitude of communication devices which allow people to access and share information, the need for at least a basic level of information security education is paramount.

Most office jobs in areas such as health information, inventory management, banking, marketing, etc. are heavily reliant on information systems, and correct, up-to-date, and secure information. Thus, for those working in professions such as these, a basic education in information security is mandatory, so that they may learn how to use these information systems in a secure manner. In today's world where nearly everyone is digitally interconnected with each other, and information sharing plays a very important role in the day-to-day life of people as they utilize the Internet for most of their activities including shopping, banking, managing their health, ordering their meals, etc. (Kim & Solomon, 2016), companies and organizations dealing with vast amounts of data and information are not the only subjects at risk of information security breaches, but any person connected to a network through a communication device of any sorts could be a victim of information security attacks (Senanayake & Fernando, 2018). Hence, it is of the utmost importance not only for those who work with critical information on a daily basis, but for anyone using information systems for any purpose, whether professional or personal, to be cognizant in information security and be aware of threats and vulnerabilities they could be faced with, and thus, to acquire at least a basic knowledge on countermeasures against these threats and vulnerabilities, so that they may securely access and share the information that they do use, in order to ensure that they utilize correct information and that their information is kept safe.

Hence, everybody requires an education in information security, regardless of their profession, or field of study. This includes not only students from science, technology, engineering, and mathematics (STEM) backgrounds, but also students from non-STEM backgrounds. Yet, as a subject area that is based on a STEM foundation, and falling directly under the STEM category, a thorough education in information security requires a STEM background with a good foundation in mathematics. However, the majority of information system users are from non-STEM backgrounds such as arts and humanities. Yet, this should not prevent them from obtaining a basic education in information security, especially when that education is crucial for their jobs and personal lives.

It is important to note that information security education could happen in varying degrees and levels, and that not every student requires the same level or depth of knowledge. While the students pursuing careers in information security, such as information security officers, network engineers and administrators, risk engineers, operations and physical security managers, policy makers, digital forensics investigators, etc. would undoubtedly require a deeper level of information security education, and would therefore require a strong STEM background in order to obtain that knowledge, the others, who require only a basic knowledge of information security so that they may be able to properly and securely access, and share the information they use, and thereby, function in this digital era without having to face any major threats in cyberspace, may obtain that basic knowledge without a strong STEM background.

Yet, as information security is a subject area which is founded in mathematics, it is undeniable that there are certain mandatory mathematical concepts that need to be studied in order to understand some subject areas and information security concepts. However, the usual bottom-up approach of first teaching those mathematical concepts so that the STEM foundation is laid on top of which the information security education can then be built, might be rather overwhelming for students from a non-STEM background. Instead, this paper proposes a top-down approach for teaching the STEM concepts behind information security to non-STEM students, allowing them to learn these mandatory STEM concepts in a more natural and practical manner stemming from day-to-day occurrences rather than deriving them through mathematical laws and processes, thereby allowing these non-STEM students to successfully obtain the basic information security education that they require.

A thorough and in-depth education in information security should cover risk assessment, access control, networking and telecommunication security including communication systems, network structures and architectures, networking devices, routing protocols, etc., cryptography, security architecture and models, physical and operations security, business continuity planning, and disaster recovery planning, etc.

(Fernando, 2018; Harris & Maymi, 2016). However, not everyone requires, nor seeks, a thorough and comprehensive education in information security, and their required depth of knowledge in a subject area varies based on the needs of the student and their intended profession. For instance, even though information security professionals who analyze security risks and implement countermeasures require a thorough understanding across all areas and domains of information security, a basic education in information security would equip most users of information and communication systems with the knowledge to protect themselves in cyberspace (Fernando, 2025). Hence, for those non-technology professionals from non-STEM backgrounds who require a basic level of information security education, so that they may have sufficient knowledge to securely access, share, and use information for their jobs and day-to-day needs, higher education programs should provide an approach to information security education that does not involve first laying down that thick, solid foundation in mathematics that is required by information security specialists and other information professionals. The next section of this paper explores some of the mandatory STEM components for certain aspects of information security education, and how a top-down approach could help in providing that education to non-STEM students.

2. Different Areas of Information Security Education and the Mandatory STEM Concepts behind them

At the beginning, information security focused mainly around technological aspects such as network security and cryptography, etc. (Bishop, 2003), but as it became obvious that the users were the weakest link and that human errors played the biggest role in information security breaches, the human aspect pertaining to information security was recognized (Fernando, 2018). As the focus of information security thus shifted from being technology-oriented to management-oriented (Lacey, 2009), international standards such as ISO/IEC 270001 (2005) etc. also emphasized the need to take human resource security into consideration when managing information security. Vroom and von Solms (2003) explain how effective information security requires not only physical and technical controls, but also operational controls, which concern the behavior and actions of users with regards to information security and are listed under security policies, procedures and guidelines. They further state that even though these policies, etc. are audited to ensure their effectiveness, the performance of users and their adherence to these policies, procedures and guidelines are simply assumed (Vroom & von Solms, 2003). Yet, people often find ways to work around such established policies, etc. instead of actually following them. This being the case, tricking people to reveal confidential information is much easier than penetrating the myriad of layers of technological security mechanisms that are put in place. In fact, most information security attacks such as social engineering, spear phishing, or willing or unwilling, knowing or unknowing collusion from an insider, etc. require a human element in order to succeed (Williams, 2011). In the abundance of misinformation and disinformation in today’s world, along with the addition of technologies such as generative AI which allow such misinformation and disinformation to be fabricated to perfection with great ease and speed, which makes it almost impossible to distinguish true facts from fabricated false information, the need for being at least somewhat knowledgeable in information security and its best practices, is paramount to ensuring that the information one uses is accurate, and that it is accessed and shared in a manner that maintains its integrity and confidentiality.

The Certified Information Systems Security Professional (CISSP) certification defines eight CISSP domains as Security and Risk Management, Asset Security, Security Architecture and Engineering, Communication and Network Security, Identity and Access Management, Security Assessment and Testing, Security Operations, and Software Development Security (Harris & Maymi, 2016). Accordingly, Fernando (2018) identifies the basic subject areas of an overall information security education as risk assessment and management (assessing potential risk factors to determine the appropriate level of security), security architecture and models (based on security requirements and priorities of an organization), security management practices (establishing and managing a security system), access control systems and methodology, telecommunications and network security, cryptography, physical security, applications and systems development security (secure software development), operations security (ensure smooth operation of routine activities to allow the system to run in a secure manner), business continuity planning and disaster recovery planning (performing business impact analysis to help recover from disasters and continue business), security laws, investigations, and ethics (components of cyber-law), and information security attacks.

Not all users need to acquire knowledge in all these information security subject areas. While information security professionals require an in-depth knowledge in these to enable them to perform risk analysis, identify countermeasures, and implement solid security practices to help protect the facility, network, system, and information, by efficiently and predictably balancing risk with service (Harris & Maymi, 2016), software engineers, other information technology professionals, and students of computer and information sciences, etc. would require an overall understanding in information security, along with further exploration of certain identified domains such as applications and systems development security, network and telecommunications security, etc.

A basic education in information security should cover the above categories briefly, while digging deeper into areas such as risk assessment, access control, network security, cryptography, and physical security, while also looking somewhat in depth at secure software development, backups, and cyber law and ethics, and attacks on information security.

The following sub sections look at these areas where a deeper understanding would be required by a basic information user:

2.1 Risk Assessment and Management

Assessing potential risk factors to determine the appropriate level of security should be discussed in brief so users will understand the proper identification of all assets (including facility, hardware, software, data, human assets, knowledge, etc.), and valuation of assets (determine the value of assets based on the cost of acquiring new assets to replace assets if lost or damaged, cost of developing/getting the assets back to original state, cost of maintaining assets, cost of lost productivity when assets are unavailable, cost of replacing corrupt or lost data, value to owners and users, value to adversaries, value of intellectual property, price others are willing to pay for it, liability issues if assets are compromised, usefulness of assets, etc.). Identifying threats to assets to determine their exposure rates and probabilities of risk should be discussed. Major risk categories include physical damage (for e.g.: fire, water, vandalism, power loss, natural disasters, etc.), human errors (i.e.: accidental or intentional action or inaction that disrupts productivity), equipment malfunction (i.e.: failure of systems and peripheral devices), inside and outside attacks (i.e.: hacking, cracking, attacking), misuse of data (for e.g.: sharing trade secrets, fraud, espionage, theft, etc.), loss of data (intentional or unintentional through destructive means), and application errors (for e.g.: computation, input, buffer overflows, etc.). How to classify threats by category and calculate actual magnitude of potential loss in order to rank severity of identified vulnerabilities and prioritize potential risks should be briefly discussed, along with how to identify possible security countermeasures to reduce identified risks to an acceptable level, and determining the suited security countermeasures through cost-benefit comparison (comparing security budget with the required protection; i.e.: the safeguard should only be implemented if the cost of loss of assets is greater than the cost of the safeguard), should be taught in brief.

2.2 Access Control Systems and Methodology

Controlling access to information based on privileges assigned to a specific user or user role should be covered.

2.2.1 Authentication to verify user’s identity/credentials

How to ensure they are who they claim to be by using: something the user knows (for e.g.: signature, password, personal identification number/PIN, passcode, key phrase, etc.), something the user has (for e.g.: key, swipe card, token, etc.), or something the user is, such as biometrics (for e.g.: fingerprint, facial scan, voice print, iris scan, retina scan, palm scan, hand geometry, hand topology, signature dynamics, keyboard dynamics, etc.) should be discussed.

2.2.2 Verifying user’s authorization to access the requested information

How to verify if the user has the need-to-know and authorization to access that information/data object based on the organization’s security model, by comparing the user’s security clearance level with the information/data object’s classification level, verify the methods or modes through which the user is allowed to access that information (for e.g.: through a graphical user interface, command line interface, direct access to the back-end database, etc.), validate what actions the user is allowed to perform on the information (i.e.: enter/input/create new information, view/read, update, or delete existing information), etc. should be discussed. The advantage of defaulting to 'no access' and allowing access only to those users that have been explicitly authorized access, rather than first allowing access to anyone who meets the criteria and then denying access to blacklisted users should be discussed (Fernando, 2018), along with the pros and cons of Single Sign-On (SSO) systems, which allow users to access many interconnected systems during the session by signing on once.

2.3 Telecommunications and Network Security

A basic information security education should talk briefly about how network structures and communication systems are designed and implemented to ensure secure communication of information. Network structure includes the architecture and design of the network and the material used for constructing it, i.e.: the type of network (wide area network, local area network, metropolitan area network, etc.), topology of the network (for e.g.: ring, bus, mesh, star topology, etc.), access technologies (for e.g.: Ethernet, token ring, Carrier-sense multiple access/CSMA with collision detection or collision avoidance, etc.), and wireless technologies (for e.g.: frequency hopping or direct sequence spread spectrum, etc.). It should look more in detail at wireless medium or cabling (for e.g.: coaxial or twisted pair copper cables, fiber optics, etc.) optimized for different parts of the network to ensure the least noise, attenuation, crosstalk, etc., fire rating of cabling material, type of transmission (whether analog or digital, asynchronous or synchronous, broadband or baseband), etc. It should briefly cover Intranets, Extranets, Network Address Translation (NAT), Internet Protocol (IP) addressing formats (i.e.: version 4 – IPv4 or version 6 – IPv6), subnets and subnet masks, firewall types (i.e.: Packet Filtering, Stateful Inspection, Application Proxy, etc.), while looking deeper at type of encryption, e.g.: link encryption (encrypt all data including headers, routing data, addresses, etc., along a communication path, requiring decryption at each hop, but providing extra protection against packet sniffers) or End-to-End encryption (where headers, addresses, routing data, etc. are not encrypted, thus eliminating the need for decryption at each hop), etc. among others.

2.4 Cryptography

The art and science of disguising data is important to be looked at in some detail so that a basic information user would know the ways of storing and transmitting data in a form that can only be read and processed by its intended users or recipients. Information can be protected by encoding/encrypting/enciphering it into an unreadable format, so as to hide it from unauthorized users. The authorized users or intended recipients of the transmitted coded message can decode/decrypt/decipher it with the proper key (Fernando, 2018). It is important to learn a little about different ciphers including substitution ciphers (where letters of the plaintext are substituted with different characters to create the cipher-text), transposition ciphers (where letters of the plaintext are scrambled to create the cipher-text), running key cipher (where the key may be hidden in the physical world and could for e.g. refer to a certain letter in a certain word in a certain line on a certain page of a certain book, etc.), and concealment cipher (where a certain agreed upon key, such as every third letter of the message, is used). Other methods of camouflaging data, such as steganography (hiding data in another media such as in an image, audio or video file.), and encryption algorithms where complex mathematical formulae are applied in a specific sequence to plain text in order to encrypt it, should be briefly discussed. How the strength of the cryptosystem depends on the encryption algorithm (the more complex the algorithm, the more difficult it is to crack, and the higher the security), the importance of the secrecy and length of the key (the longer it is, the more difficult it is for an adversary to guess it), etc. should be emphasized. The stronger the cryptosystem, the more effort is needed to break it. A cryptosystem is considered strong if it is still secure when the encryption algorithm is made public and only the key is kept secret. Stream ciphers perform mathematical functions on individual bits in a stream (where a key determines which functions are applied in what order), whereas block ciphers divide the plaintext message into blocks of bits and perform substitution, transposition, and other mathematical functions to it (where the algorithm dictates the functions to be used and the key dictates the order in which they should be used). Cryptosystems and their use of keys should be explained in somewhat detail to ensure the required strength and secrecy of keys are properly understood. For instance, the use of symmetric keys (same key for decrypting as for encrypting) or asymmetric keys (different, but related key for decrypting than for encrypting), should be discussed. Symmetric keys are faster than asymmetric keys. By having a private key and public key combination (where the private key is secret and known only to its owner, and the public key is known by other users) asymmetric keys are much more secure, but carry significant overhead and are slower compared to symmetric keys. In addition to added security (by not sharing the private key), asymmetric keys also enable verification of sender's identity as the sender's private key acts as the sender's signature. In order to both ensure security and verify sender's identity, the message will have to be encrypted twice (once using the sender's private key and once using the receiver's public key) and also decrypted twice (using the receiver's private key, and the sender's public key). Double encryption and double decryption add further overhead to the performance of asymmetric keys, but also verify the identities of both parties in a secure communication. Hybrid methods utilize both symmetric and asymmetric keys to get the best of both worlds, by encrypting a symmetric session key using secure asymmetric keys, and then using the faster, symmetric session key for both encrypting and decrypting messages communicated within that session (thereby making the communication faster and more efficient due to lack of extra overhead), and then destroying that session key at the end of the communication session (to ensure further security). Public Key Infrastructure (PKI) which uses the services of a Certificate Authority (CA), a trusted third party, to vouch for the trustworthiness of parties (especially servers) included in communication (especially in client-server communications), by issuing a certificate verifying their identity, should be discussed to emphasize the importance of understanding warnings about messages from an unverified sender, etc. It is important to have some understanding about the concept of hashing, a form of one-way encryption (where decryption is not possible, but message integrity can be verified by comparing against the original hash/message digest), to know that password files should be stored in either encrypted or hashed form. It is best to hash the passwords and store the hash instead of the password itself (Fernando, 2018). Then, each time the user enters their username and password combination, the entered password will be hashed and this hash will be compared against the stored hash corresponding to the entered username. If it is exactly the same, then the entered password is correct (as the smallest change to the plaintext will make a significant change in the hash) and the user is authenticated. A hash value encrypted with the sender's private key creates their digital signature. Cryptanalysis, the science of studying and breaking the secrecy of encryption algorithms, should be looked at in brief. Frequency analysis compares the most frequently used letters and words in the cipher-text to those in the alphabet of the plaintext, to figure out patterns and thereby figure out the key and break the cipher. The importance of key management should be taught. Keys need to be securely distributed (protected during transmission, etc.) to the correct entities and continuously updated. Key Escrows help by maintaining back-up keys in case they need to be recovered. Multiparty control of emergency keys, where two or more keys from two or more different parties are required, reduces potential for abuse (Fernando, 2018).

2.5 Physical Security

The physical elements contributing to information security should be discussed. For instance, securing the perimeter and restricting access to secure areas within the facility, Closed Circuit Television (CCTV), motion detectors, sensors, alarms, security guards, fences, walls, etc. help enforce perimeter security and physical access control. Monitoring activities, examining devices taken inside and outside of the facility, signing out material, etc. help to reduce and deter theft of physical items. Intrusion detection systems (for e.g.: proximity detection, photoelectric/photometric detection, wave pattern detection, passive infrared/IR, acoustic-seismic detection, electromechanical detection, vibration detection, etc.) and intrusion prevention systems help to detect and deter intruders. Alarms should notify law enforcement officials of intrusions. Another area which should be taught at some depth is regarding authorization methods and controls, such as biometrics, individual access badges, magnetic swipe cards, wireless proximity readers (recognizing presence of approaching object), and tokens, etc., which add extra layers of security, and thereby multiple barriers that need to be circumvented in order to access resources. Proper facility construction should be looked at in brief to understand the requirements for protecting the facility and its human assets from fire and water damage, proper heating, ventilation and air-conditioning (HVAC) controls, antitheft mechanisms, etc. Main threats to physical security include theft, interruption of services, physical damage, compromised system integrity, unauthorized information disclosure, etc. Placement of doors, windows, secure hinges, fire rating, resistance to forcible entry, directional opening (opening out from the facility), electric locks reverting to disabled state for safe evacuation in power outages (if a 'safety first' approach is followed), bulletproof/shatterproof glass, etc. load and weight bearing floors and ceilings, non-conducting surfaces and anti-static flooring, eliminating drop ceilings so intruders cannot lift ceiling panel and climb over partitioning walls, proper placement of water and gas lines, shut-off valves, positive flow (where material flows out of and not into the building), positive air pressure in HVAC systems, protected intake vents, dedicated power lines, emergency shut-off valves and switches, and their proper placement, etc. should be briefly discussed. Fire detection and suppression through proper placement of the type of sensors and detectors best suited for the task or place (i.e.: smoke activated, heat activated, or flame activated) and sprinklers (for e.g.: wet pipe, dry pipe, pre-action, deluge, etc.), alternatives to sprinklers such as to shut down air circulation, use carbon dioxide (CO_2), and alerting the fire station, etc. should be discussed, along with the importance of illuminated and visible exit signs and unblocked fire exit doors to ensure safe evacuation in emergencies, and regular monitoring of HVAC controls, climate controlled atmosphere, and reduced contaminants (corrosion, blockage, hazardous gases, etc.). Location, visibility and accessibility of facility should be discussed in brief. For instance, natural camouflage vs. attracting intruders, likelihood of natural disasters, construction material (fire protection/combustibility levels), load borne by walls, beams and columns, reinforcement for secured areas, implementation of physical controls such as fences, gates, locks, lighting, etc. should be considered before building the facility. Location of facility components is important. Data centers should not be located in top floors (in case of fire) or in basements (in case of floods), but at the core of the building where there is easy access to emergency crews. Secure assets should be located in semi-secluded areas with limited accessibility. Computer and equipment rooms should be located near wiring distribution centers, and having only a single access door so it is impossible to access through public areas. Back-up and alternate electrical power supplies should be discussed so users know the back-up procedures in cases of power loss (as disabled Intrusion Detection Systems make intrusion easier). A clean and steady power source (without interference or line noise, fluctuation, electromagnetic interference/EMI, radio frequency interference/RFI, or transient noise.), and proper placement of distribution panels and circuit breakers to allow easy access are important, as are surge protectors, orderly shutting down of devices, power line monitors, regulators, grounded connections, shielded lines (magnetic induction), three-prong connections and adapters. Fluorescent lights should be avoided to eliminate RFI, and one should avoid plugging outlet strips and extension cords to each other, etc. Another important factor to teach at some detail is locking mechanisms. Cipher (programmable) locks such as door delays (alarms triggered if held open too long), key-override (special key combination for emergencies overrides normal procedure), master-keying (supervisory personnel can change access codes), and hostage alarm (key combination alerting guards/police when under duress), etc. increase security. Device locks for hardware include switch controls (covering on/off switches), slot locks (mounted bracket and steel cable securing system to stationary component), port controls (blocking access to drives and unused serial and parallel ports), peripheral switch controls (on/off switch between unit and slot), and cable traps (prevent removal of input and output devices by passing cables through lockable unit), etc. Other measures such as weight detectors to prevent piggybacking (entering through a door that was opened for another person), and the importance of auditing physical access (date and time of access attempt, entry point, user identification, unsuccessful attempts, attempts at unauthorized times, etc.) should be covered.

2.6 Applications and Systems Development Security

Any user who might also develop information systems or applications would need an understanding about secure software development. Information security should be integrated into the software development life cycle beginning with the requirements gathering phase (identify required level of security), moving on to the analysis and design phase (incorporate suitable security measures in the software design), through to the implementation phase (develop the designed security features), testing and debugging phases (also test security mechanisms for accuracy and correctness), deployment phase (configure security mechanisms properly), all the way through to the maintenance phase (constantly test, assess and update security mechanisms to suit current security needs). Multiple layers of software security are needed, starting with the front-end user interface (validate user input to filter out invalid input or malicious code), through to the back-end database (screen and parse data before inserting it into the database). Proper separation of user roles through the software system's user interface by only enabling and making visible the options for functionality that particular user or user role is authorized for is important. Not seeing other functionality available only to other users is an extra layer of security as not knowing about their existence helps limit users only to functionality that is allowed to them.

Options should be provided for users to select input from (i.e.: radio buttons, check boxes, drop-down menus, etc.) whenever applicable to reduce possible input errors. Adopting best practices for programming/software development to ensure no room has been left for unforeseen security breaches, closing back-doors/maintenance hooks (i.e.: alternate channels created by programmers to enable easy testing of the module instead of navigating through the proper access path each time) and other covert paths, which, if remained opened, would also allow unauthorized users access to the system, checking for other programming loopholes which could lead to information security problems/breaches (for e.g.: buffer overflows, which can be exploited to enter lengthy inputs which overflow the buffer's boundaries and overwrite other memory locations adjacent to it, etc.) should be covered.

2.7 Business Continuity Planning and Disaster Recovery Planning

How business impact analysis is performed to help recover from disasters and continue business should be briefly discussed so that users know about different back-up and recovery alternatives. For instance, concurrent/simultaneous soft back-ups such as to a Redundant Array of Inexpensive Disks (RAID), allow quick recovery to the latest data/information, while frequent back-ups to storage media kept in a different location (within the facility) from the servers and other system resources allow somewhat fast recovery to recent data/information. Less frequent, periodic hard back-ups where storage media is moved to a different location outside the facility, allow recovery (albeit not to the most recent data/information) from disasters which destroy the facility.

2.8 Security Laws, Investigations and Ethics

A brief understanding of the different components of cyber-law is needed. Users should be educated on security laws, regulations and ethics by which they should abide, liability and ramifications of actions, surveillance, search, seizure, and intrusion of privacy, etc. It is important to teach them that constant surveillance or monitoring of user activity, which may be required at times, might intrude on user's privacy and not be very ethical.

2.9 Information Security Attacks

It is important for all users of information and information systems to know about different methods and forms of attacks, and possible countermeasures. Eavesdropping, network sniffing, wiretapping, intercepting/capturing data passing over the network, etc., are passive attacks, where the attacker is not affecting protocol, algorithm, key, message, or encryption system (Fernando, 2018). Passive attacks are hard to detect, thus should be prevented rather than detected. Passive attacks are usually for reconnaissance before an active attack. Altering messages, modifying system files, masquerading/spoofing, etc., are active attacks, where the attacker does something with the gathered data instead of simply reading it. Tools such as protocol analyzers, port scanners, operating system (OS) fingerprint scanners, vulnerability scanners, exploit software, war-dialers, password crackers, keystroke loggers, etc., and malicious software such as viruses, worms, Trojan horses, rootkits, spyware, etc. could be used in information security attacks. Access control monitoring helps to keep track of attempts to log in (especially unsuccessful attempts), and thereby help identify any intrusion attempts. It is important to talk about honey pots, which are open (not locked-down) computers with their services enabled, but with no real company information, used to entice would-be attackers, and how enticement does not induce an attacker to commit the crime and is thus, legal. Entrapment, however, is inducing to committing a crime, and is thereby unethical and illegal. It is important to teach about some of the more common information security attacks such as man-in-the-middle, denial or service (DoS), distributed denial of service (DDos), dictionary attacks, brute-force attacks, phishing, spear phishing, pharming, phreaking, social engineering, replay attacks, keystroke monitoring, shoulder surfing, etc. so that the users may know to avoid falling victim to these threats.

As previously stated, information security is a subject area that is based on a STEM foundation. Risk and uncertainty are difficult concepts for people to evaluate (West, 2008), and the human brain perceives security somewhat differently from its reality (Schneier, 2008). The reality of security is mathematical, based on the probability of different risks and the effectiveness of different countermeasures, while the feeling of security is based on each individual person's psychological reactions to these (Schneier, 2008). This divergence between the reality and the perception of security leads to gaps between the required and implemented security countermeasures, where if the threat is perceived to be greater than what it actually is, one can feel paranoid even when they are secure, whereas when they fail to comprehend the real intensity of the risk they may become complacent and undermine it, thereby increasing their vulnerability to attacks (Fernando, 2018). Humans make trade-offs intuitively, exaggerating some risks or costs, while downplaying others (Schneier, 2008). West (2008) states that humans tend to believe that they are less at risk and maintain an acceptable degree of risk in their minds by increasing risky behavior to suit increased security measures, thereby resulting in prioritizing security only when they start to have problems with it. Therefore, an important part of information security education is teaching users that anyone could fall victim to an information security attack at any time. Hence, another essential component of any information security education is information security best practices (Fernando, 2018), as listed in table 1 below:

Table 1. Information security best practices

Best Practice	Description
Separation of tasks	Separating work-related tasks from personal tasks: ensure only work-related cyber behavior will be monitored.
Password security behavior	Adopt strong and long passwords with special characters, numbers, both uppercase and lowercase letters, which are not obvious and are difficult to guess. Change passwords frequently. Avoid reusing former passwords. Avoid saving, writing down, or storing passwords in places easily accessible to others. Avoid incorporating personal information that can be easily found within one's password. Avoid sharing the same password across different applications, or with others.
Data back-up behavior	Perform frequent and periodic data back-ups in multiple forms and in multiple storage media to enable recovery of data if needed.
Data sanitization behavior	Ensure that unnecessary copies (both hard and soft copies) of data are destroyed. Regularly sanitize external storage media. Control access to personal storage media by others, and minimize using storage media belonging to others. Periodically delete temporary files, cookies, browsing history, saved passwords, etc.
Network security behavior	Ensure that firewalls are enabled. Periodically update antivirus software and scan computer disks and drives. Check for authenticity of websites, e-mail attachments, etc. Validate credentials of the other party before correspondence.
Physical security behavior	Be aware of the surrounding. Lock computers when leaving the desk. Lock cupboards, desks, office, home, vehicle, etc. Ensure that confidential or personal items are not left unattended. Avoid sharing personal items whenever possible. Avoid using unknown items without validation.

When teaching these subject areas, we see that there are certain mandatory STEM concepts that need to be taught in order to help the students properly understand these information security concepts. These information security concepts and their mandatory STEM concepts are listed in table 2 below:

Table 2. Mandatory STEM concepts behind information security education

Information Security Concept	Mandatory STEM Concept
Risk assessment	Arithmetic, algebra
Network security	Basic geometry, arithmetic, binary numbering
Cryptography	Arithmetic, algebra, binary and hexadecimal numbering
Physical security	Basic geometry, arithmetic
Data backup media	Binary numbering
Password security	Arithmetic, algebra

As seen above, students of information security would require knowledge of STEM concepts such as basic arithmetic and algebra in order to perform a basic risk assessment and cost-benefit analysis, and to demonstrate how long a computer or a supercomputer will take to crack a password of certain length, containing characters from a given set of characters, through brute-force, and therefore determine the length of a password and what type of characters should be incorporated in it, etc. Some basic knowledge of geometry will be beneficial, along with arithmetic, when calculating the distance from a networking device to a computer, or for determining the best location for a certain device, etc. with regards to both network security and physical security. Further, the knowledge of binary numbers would be of high importance, as concepts such as digital memory for data storage media, cryptography, and networking utilize binary numbers in multiple ways (Fernando, 2025). For instance, binary addition, subtraction, shift, etc. are often used as parts of a cryptographic key when encrypting a message, while network packet headers are created in binary form, where each bit or each set of bits represents a certain element. Binary and hexadecimal numbering is also used when creating internet protocol (IP) addresses – both IPv6, and the previous version, IPv4, as well as the subnet masks used to identify the subnets that each device in a network belongs to in the IPv4 network addressing scheme (Harris & Maymi, 2016, Fernando, 2025).

While there are other areas in information security where we dive deeper into more mathematical concepts such as network routing protocols, which would entail looking at multiple different routing algorithms which in turn would require a thorough knowledge of mathematical data structures and their properties, trigonometry, and calculus, or elliptical curve systems used for cryptography, which would require a deep understanding of geometry, etc., as this paper focuses on basic information security education aimed at non-STEM students who would be information users and not an intensive education in information security aimed at information security and technology professionals, those intense subject areas which require a solid, deep understanding of mathematical and STEM concepts will not be covered here.

The next section will look at how some of these mandatory STEM concepts behind information security education can be taught in a top-down fashion so as to allow students from non-STEM backgrounds to easily comprehend these concepts.

3. Top-Down Approach of Teaching Mandatory STEM Concepts behind Information Security

When providing a basic education in information security to basic information users, who are mostly from non-STEM backgrounds, if these mandatory STEM concepts identified above are taught in the usual bottom-up fashion, where you first teach these STEM concepts to lay the required mathematical foundation, and then start teaching the information security concepts, these non-STEM students could easily be overwhelmed by theoretical concepts for which a practical application might not seem obvious to them (Fernando, 2024). This could lead to unnecessary confusion and frustrations and could eventually result in an unsuccessful pursuit of education. On the contrary, in the top-down approach proposed here, the information security concepts are taught first, and when it comes to the point where we need to delve deeper, the STEM concepts are introduced in a natural and practical manner based on already familiar examples, so that these non-STEM students can comprehend these concepts better. Further, as this top-down approach allows you to go only as deep as you need to go, you do not need to go into more detail or depth than necessary when teaching the required mathematical concepts, but can limit it to only the mandatory STEM concepts required to provide that basic education in information security.

The rest of this paper will look in more detail as to how this top-down approach could be utilized for teaching certain STEM concepts identified above.

As binary and hexadecimal numbering is required by multiple information security subject areas, the next subsection of this paper will examine how to utilize a top-down approach to teach these STEM concepts to non-STEM students.

3.1 Teaching Binary and Hexadecimal Numbering Systems using a Top-Down Approach

The bottom-up method of teaching binary numbering utilizes long division to convert a decimal (base 10) value to a binary (base 2) value. Although this is a very simple calculation for any STEM student, long division is an area where most non-STEM students struggle with, and if binary numbering is introduced in this manner, there is a good chance that non-STEM students might get overwhelmed and frustrated and avoid binary numbering altogether (Fernando, 2025). Yet, as binary numbering schemes are used in so many information security subject areas, even a basic education in information security requires some understanding of binary numbering.

Instead of addressing binary systems directly, however, the top-down approach would first describe how and why binary systems are required. For instance, we can teach these students that each character is depicted in computers using Unicode, which is a binary number, that is depicted in hexadecimal (base 16) for ease of use. For example, the Unicode for uppercase ‘A’ would be 01000001, while the Unicode for lowercase ‘a’ would be 011000001, and the Unicode for asterisk ‘*’ would be 00101010. We can also look at another instance where binary numbers are used: when data packets are transmitted through a network, the entire message is ultimately written down as 1’s and 0’s and transmitted as that. In addition to the message, the packet also contains a header which includes the origin and destination addresses, the type of protocols to be used, and other such information, all of which is written as 1’s and 0’s, before being enveloped or encrypted for secure transmission. However, as we all know, there are many instances when such packets get intercepted by those other than the intended recipient. Even if it were not intercepted, noise, electrical spikes and other such problems could lead to data packets being corrupted. And so, there are many ways such as encryption, hashing, etc. which allow us to check to see if the data packet was tampered with or corrupted in any way. One of the most basic and less efficient ways to do this is to include a parity bit, which is also called the checksum bit, in the packet header. In this method, you count the number of 1’s in the string of data consisting of 1’s and 0’s, and you include an additional parity bit to even out the number of 1’s. So if there was already an even number of 1’s in the data string, such as 11011, then you add 0 as the parity bit to retain the even number of 1’s, whereas if the number of 1’s in the data string was odd, such as 10011, then you add 1 as the parity bit to even out the number of 1’s. When this message is received by the recipient, they will check to see if their data packet arrived with an even number of 1’s, and if so, they will remove the parity bit and utilize the data string as needed. But if their data packet arrived with an odd number of 1’s, then they know that the data packet was corrupted during transmission and would discard it. The obvious problem with this system is that, if someone intentionally wants to tamper with the data packet, they can make sure to change the bits so that it ends up with an even number of 1’s including the parity bit anyway, and so, this is not a very efficient way of sensing if the data packet was tampered with or corrupted. However, as an instance of where binary numbers are used, the parity bit is certainly worth mentioning. First teaching the students these instances where binary numbering is used, will make them more open to learning about them.

Next reminding these non-STEM students that they might already be somewhat familiar with some of these binary or hexadecimal codes, would be a good point of entry to ease into this otherwise feared topic of binary and hexadecimal numbering. For instance, another practical application of binary and hexadecimal numbering that would appeal to these students would be how the RGB color system assigns codes to each color red, green, and blue from 0 through 255 in order to figure out the required saturation of each of these colors to create the required color. And even these non-STEM students might be somewhat familiar with the hexadecimal codes such as #FF0000 for red, #00FF00 for green, #0000FF for blue, #FFFF00 for yellow, etc.

Having first spoken of some of their uses, this top-down approach can then move on to teaching these students how to convert decimal numbers into binary and hexadecimal numbers, so that they can then make sense of these codes that they are familiar with, but did not exactly know what they represented, such as what the letter F represents in an RGB color code (Fernando, 2025).

Having first piqued their interest in these binary and hexadecimal numbering schemes, and having emphasized their importance, the next step would be to teach these non-STEM students how these numbering schemes are created. Obviously, a binary numbering scheme means that instead of working with decimal, as in with the numbers 0,1,2,3,4,5,6,7,8,9, and then counting in 10's, we will simply be counting using the numbers 0 and 1. Instead of leaping into long division to convert a decimal number into its binary value straight away, the students should be reminded that different numbering schemes are not something they are unfamiliar with. The best example is that of time (Fernando, 2025), where we count from 0 through 59 seconds, and then once it reaches 60, instead of stating 60 seconds, we simply state 1 minute. Similarly, we count up to 59 minutes, and then beyond that, the 60th minute would be 1 hour. After 23 hours and 59 minutes and 59 seconds, the next second makes it 1 day, and so on. In addition to time, there are other instances when we differ from our usual decimal counting scheme, such as distance and weight. For instance, when we look at distance, the 12th inch makes 1 foot, 3 feet make up a yard, etc. Similarly, the 16th ounce makes 1 lb, etc. This will show students that they are already familiar with multiple different numbering systems which they use in practice, even though they do not consciously make these conversions (Fernando, 2025).

Figure 1, below, depicts how we go from 0 to 9 in decimal counting, and then how 10 is formed by resetting our rightmost digit back to 0 and adding a second digit to the left as 1 to form '10'.

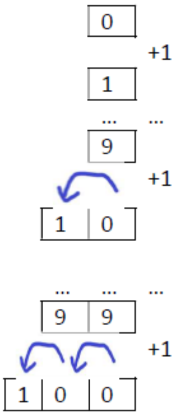

Figure 1. Decimal (base 10) counting system

Note that once that second digit from the right as well as the rightmost digit are filled up to 9 to give us 99, and we no longer have any numbers left to go on those two digits, then we reset those two digits to 0 and add a third digit to the left as 1 to form '100', and so on (Fernando, 2025). This top-down method also shows how to perform these conversions by visualizing containers for the rightmost digit and each digit to the left thereafter, instead of worrying about long division.

3.1.1 Binary Number System

We then teach that in binary, as we only have the numbers 0 and 1 to work with, we count to 0, then 1, and then when we need to go another number higher, similarly to what was shown above, we reset that rightmost digit to 0 and then add another digit to the left and set that to 1 to create 10. However, in this case, as this is binary and not decimal, this binary 10 stands for the value 2 instead of the decimal value 10 that we are familiar with (Fernando, 2025). This is depicted in figure 2 below.

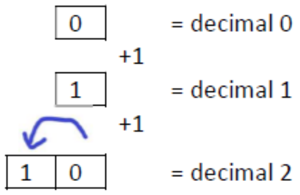

Figure 2. Binary (base 2) counting system

This method will be continued further to demonstrate that adding 1 more to binary 10 will make it binary 11, which is equal to decimal 3 (as shown in figure 3), and adding another 1 to binary 11 will make it binary 100, which is equal to decimal 4, and so on, as depicted in figure 4.

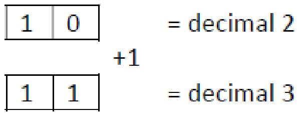

Figure 3. Counting to binary 11 (decimal 3)

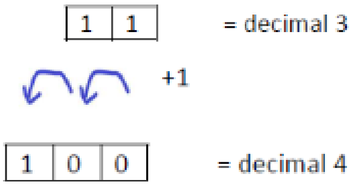

Figure 4. Counting to binary 100 (decimal 4)

Then, looking at the instances when a new digit is created, we can show them that in the decimal system, a new digit is created at 1, 10, 100, 1000, etc., where we see that $1 = 10^0$, $10 = 10^1$, $100 = 10^2$, $1000 = 10^3$. This shows that whenever we go up a power to the 10 is when we create a new digit to the left in the decimal system. We then show that it must also hold true in the binary system, where each time we go up a power to the 2, as in: $2^0 = 1$, $2^1 = 2$, $2^2 = 4$, $2^3 = 8$, $2^4 = 16$, etc., we would create a new digit to the left, as shown in table 3.

Table 3. Binary numbers which create new digits

Binary	Decimal
1	1
10	2
100	4
1000	8
10000	16
100000	32
1000000	64

10000000	128

This would also reveal a very important number series, that of the series of numbers of the power of 2, which is 2^0, 2^1, 2^2, 2^3…., i.e., the series: 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1024, 2048, 4096, etc. We can then remind the students that they are already somewhat familiar with this series, as they have noticed that memory such as computer memory or SD cards have the values 32 GB, 64 GB, 128 GB, 256 GB, etc., and emphasize that this is due to the fact that computer memory, works in binary, and that that is why it is called digital memory: as it contains 2 states, that of either 1 or 0 (Fernando, 2025).

3.1.2 Hexadecimal Number System

We can then move onto hexadecimal numbers which are of base 16. As $16 = 2^4$, converting a binary number into hexadecimal can be done by separating the binary number into segments of four digits each starting from the right and moving to the left, and then figuring out the hexadecimal value for each segment. For instance, binary 11101001 can be separated into the two segments of 1110 and 1001, and then the hexadecimal values for each segment can be considered (Fernando, 2025).

For the hexadecimal numbering scheme, we can use the values 0 through 15, but as there is no single digit to represent the double-digit numbers of 10, 11, 12, 13, 14, and 15, we use the uppercase letters A through F to represent 10 through 15 in hexadecimal numbering scheme as shown in table 4 below.

Table 4. Representing double-digit decimal numbers in hexadecimal

Decimal	Hexadecimal
10	A
11	B
12	C
13	D
14	E
15	F

Hence, the two binary segments of 1110 and 1001 above, will be represented as E (decimal 14) and 9 in hexadecimal, to make binary 11101001 equal to hexadecimal E9. Similar to any other numbering system, when you reach value 16 in hexadecimal, as the rightmost hexadecimal digit is full at F (decimal 15), we reset that to 0 and add a new digit to the left as 1, to represent decimal 16 as hexadecimal 10. This makes decimal 17 equal to hexadecimal 11, and so on. Hexadecimal FF is equal to decimal 255, and once we reach decimal 256, which is equal to 16^2, we denote that as 100 in hexadecimal. At this point, we can remind the students about the RGB color codes which contained values such as #FF0000 for red, #00FF00 for green, and #0000FF for blue, which can also be translated into decimal as 255-0-0 for red, 0-255-0 for green, and 0-0-255 for blue. We can thereby show them that the saturation of each color could go from 0 through 255, which when converted to hexadecimal is what gives us these RGB color codes containing the # symbol followed by six hexadecimal digits which could include 1 through 9 and A through F (Fernando, 2025).

Once this is taught, if needed, we can then teach students how to convert a decimal value to binary or hexadecimal by performing long division. Once again, it is important to note that in this top-down method, you only need to go down as deep as needed, and if more intense mathematics is not required, then you do not need to go into those details that might overwhelm non-STEM students (Fernando, 2025). Approaching this vast, yet important, STEM concept of binary and hexadecimal numbering in this top-down method would allow even non-STEM students who are not used to intense mathematics to understand these mandatory mathematical concepts behind information security.

Algebra is another mathematical concept which is required for multiple information security subject areas such as risk assessment, networking, password security, etc. So the following subsection will examine how a top-down approach could be utilized to teach the mathematical concept of algebra to non-STEM students.

3.2 Teaching Algebra using a Top-Down Approach

The bottom-up method of teaching algebra would be to begin with mathematics, where you would derive algebraic equations through mathematical principles. In this top-down approach, on the contrary, we can start by showing how an algebraic equation might help in demonstrating, for instance, how to determine the required length of a password based on how long it takes a computer or a supercomputer to crack that password using a brute-force attempt.

For instance, if a modern day computer of 2.8 GHz takes $1.7 * 10^{-6}$ s (0.0017 milliseconds) to compute a hash using SHA 512, and a supercomputer or a botnet with 100,000 computers can compute the same hash in 1/100,000th of that time, then, if we consider the possible number of password combinations to be C, the number of possible characters in the password (character set) to be P, and the length of (number of characters in) the password to be L, these values can be denoted in the algebraic equation: C = P^L = P^L.

Assuming that a given password will be cracked after half of the possible passwords are checked, the following formula shows how long it takes a modern day computer to crack a password based on its length and character set, where: the time taken to crack a password (T) would equal the time taken to compute a hash multiplied by the possible number of password combinations.

Given the facts above, the time taken by a modern-day computer to crack a password is given by:

$T = [(1.7 * 10^{-6}) * (P^L)]$ s / 2

And the time taken by a supercomputer to crack a password is given by:

$T = [(1.7 * 10^{-6}) * (P^L)]$ s / (2 * 100,000)

By looking at some examples, we can see that the time taken to crack an 8-character password, which consists only of lowercase and uppercase English letters (total possible characters being 52), by a modern-day computer would be:

$T = [(1.7 * 10^{-6}) * (52^8)]$ s / 2 = 45440769.2517 s = 525.934 days

And that if we expand our total character pool to include the numbers 0 through 9, then the time taken to crack an 8-character password, which consists only of lowercase and uppercase English letters and numbers 0 through 9 (total possible characters being 62), by a modern-day computer would be:

$T = [(1.7 * 10^{-6}) * (62^8)]$ s / 2 = 185589089.747 s = 2148.022 days.

Whereas, when adding the 18 special characters to our character pool, which expands the character pool to 80, the time taken to crack an 8-character password, which consists of lowercase and uppercase English letters, numbers (0 through 9), and special characters, totaling a character set of 80 characters, by a modern-day computer would be:

$T = [(1.7 * 10^{-6}) * (80^8)]$ s / 2 = 45.220 years,

while the time taken to crack a 10-character password, which consists of lowercase and uppercase English letters, numbers (0 through 9), and special characters, totaling a character set of 80 characters, by a supercomputer would be:

$T = [(1.7 * 10^{-6}) * (80^{10})]$ s / 2 * 100,000 = 91268055.04 s = 2.894 years.

Depicting these ideas which are more comprehensible to students as algebraic equations, allows them to appreciate the need for gaining knowledge in algebra in order to better understand these information security concepts. Once this realization has been achieved, then basic algebra could be introduced to these non-STEM students in a top-down fashion using word problems to create simple algebraic equations, which they will then be taught to solve. Once again, as before, you only need to go as deep as required, and do not need to go any deeper than necessary to avoid overwhelming these non-STEM students with difficult mathematical and STEM concepts.

4. Discussion

The commonly practiced method of teaching information security is the bottom-up approach, where the first step is to teach the mathematical concepts that lay the STEM foundation, so that the education of information security can be built on top of that. While this method is straight forward, and perfectly well-suited for students from a STEM background who have an aptitude for mathematics, and while this is the preferred method for students who plan to become information security and technology professionals as they require an in-depth understanding of the theory of information security, so that they may, themselves, create such information security systems, fix system issues, or invent new techniques in the future, such a deep level of understanding of information security and technology and the theory behind it might not be required by most general information users. Instead, laying a thick mathematical foundation as in a bottom-up approach might lead to non-STEM students being overwhelmed by theoretical concepts for which a practical application might not seem obvious to them. This could lead to these non-STEM students who wish to obtain a basic education in information security being confused and frustrated, and eventually, unsuccessful in their pursuit of education. This paper discusses how utilizing a top-down approach, instead of the usual bottom-up approach could prevent the above scenario and enable these non-STEM students to successfully obtain their basic information security education.

Even though it might seem like stripping down the education in information security, so as to avoid teaching these non-STEM students the mathematical and STEM concepts behind it, is a lazy approach, this is not actually the case. Angell and Demetis (2010) discuss how linearity (one thing after another) is a delusion in this non-linear world. Thus, it can be construed that, as long as it is only a basic level of education, it is not mandatory for an information security education to be built upon a full, solid foundation of mathematics. As at least a basic education in information security is required by everyone who uses, access, or shares information, it is of utmost importance that there are education programs which provide this education not only to those who have an aptitude towards STEM subjects, but also provide the means for students from non-STEM backgrounds to obtain a basic education in information security.

5. Conclusion

In conclusion it can be stated that information security education is required by all students, but in varying levels or degrees. A complete and thorough education in information security, which also requires a thorough and solid foundation in STEM concepts will only be required for students intending to become information security professionals such as information security officers, network administrators, cryptographers, etc. Yet, any non-technology professional who uses information systems – information users – should have at least a basic education in information security so that they may know how to access and share the information they use in a secure manner, so that they may keep their personal and work-related information safe. As most of these information users may come from a non-STEM background, gaining a deep understanding and complete knowledge of the STEM concepts on which information security is rooted, may be overwhelming, and the usual bottom-up approach to teaching information security by first laying a mathematical foundation may be unsuccessful. However, by providing information security education in a top-down approach and teaching the basic STEM components required for the information security subject areas taught in a practical and natural manner as needed, non-STEM students would be able to successfully obtain the basic information security education sufficient for their non-technology professions, and personal lives. Thus, it can be concluded that information security education for non-STEM students should be provided using a top-down approach.

References

Angell, I. O., & Demetis, D. S. (2010). *Science's first mistake*. Bloomsbury Academic.

Bishop, M. (2003). *Computer Security – Art and Science*. Boston, MA: Pearson Education.

Fernando, S. (2025). Educating non-STEM students in information science and technology using a top-down approach to teach the required STEM concepts. In M. Ozkaya, & S. Alan (Eds.), *Current Academic Studies in Education and Technology* (pp. 75-104). ISRES Publishing.

Fernando, S. (2024). Information science and technology education for non-STEM students: A top-down approach. In Proc., *International Science and Technology Conference 2024* (pp. 416-423).

Fernando, S. (2018). The different aspects of information security education. In Z. Fields (Ed.), *Handbook of research on information and cyber security in the fourth industrial revolution* (pp. 182-204). Hershey, PA: IGI Global.

Harris, S., & Maymi, F. (2016). *CISSP all-in-one exam guide* (7th ed.). New York, NY: McGraw-Hill Education

ISO/IEC 270001. (2005). *Information technology – Security techniques – Information security management systems – Requirements*. Geneva, Switzerland: ISO.

Kim, D., & Solomon, M. G. (2016). *Fundamentals of Information Systems Security* (3rd Ed.), Burlington, MA: Jones & Bartlett Learning.

Lacey, D. (2009). *Managing the Human Factor in Information Security: How to win over staff and influence business*. West Sussex, England: Wiley.

Schneier, B. (2008). *The psychology of security*. Retrieved August 5, 2012, from http://www.schneier.com/essay-155.html

Senanayake, T., & Fernando, S. (2018). Information security education: Watching your steps in cyberspace, *The online journal of science and technology, 8*(2), 96-101.

Vroom, C., & von Solms, R. (2003). Information security: Auditing the behavior of the employee. *IFIP TC11 18th International Conference on Information Security (SEC2003)*, Athens, Greece. In Gritzalis, D., De Capitani di Vimercati, S., Samarati, P. and Katsikas, S. (Eds.), *Security and Privacy in the Age of Uncertainty* (pp. 401-404). Norwell, MA: Kluwer Academic Publishers.

West, R. (2008) The psychology of security. *Communications of the Association for Computing Machinery, 51*(4), 34-41.

Williams, B. R. (2011). Do it differently. *Journal of Information Systems Security Association, 9*(5), 6.