What for safeguarding this kind of information that

Business, Accounting

What is the impact of Information Technology Security onorganizations, government, and military services? The objective is tounderstand what the necessary steps in cyber-attack prevention are. Anotherobjective is how to prevent or recover from an information breach. The purposeof this paper is to examine how information security impacts U. S.

MilitaryServices, government, and large-scale organizations. In today's modern culture, technology has become a powerful asset of daily lives and continuouslyprogresses. Technological advances have flourished in impacting our lifestyle inevery sector.

Technology is utilized in energy, healthcare, education, transportation, agriculture, and more. However, with greater innovation comes agreater threat to breaches in personal information. Cyber-attacks have becomeeminent threats towards big business, military services, and the nation'sgovernment.

I. T. (Information Technology) security prevents delicateinformation such as social security, credit cards, passwords to emails andsocial media, etc., from being stolen or accessed by unauthorized users. . B. BackgroundInformation Technology Security is the process ofimplementing measures and systems designed to securely protect and safeguardinformation utilizing different forms of technology developed to create, store, use and exchange such information against any unauthorized access (IT SecurityResources, 2015).

As the internet continues to evolve, so does cybercrime. Theworldwide web has granted people access to vast amounts of information whilealso making

tasks including, shopping, banking and paying bills convenient (Comodo, 2017). Security analysts are responsible for safeguarding this kind ofinformation that is confidential to any individuals or personnel within anorganization. Panda Security detected and neutralized more than 84 million newmalware samples throughout 2015 (Panda Security, 2016). In the event of aninformation breach, the first step is to understand the nature and severity ofthe threat and the potential damage that it can cause. II.

Information Security's role in NationalDefenseThe United States Military overseasprotecting top secret information that must remain confidential such as trooplocations, launch codes, and other data (NCI, 2015, para. 3). " Before and duringthe Gulf War, hackers from the Netherlands penetrated computer systems at 34American military sites on the internet, including sites directly supportingOperation Desert Storm/Shield" (Denning, 2003 p. 5). Files containing the exactlocation of troops, their weapons, the capabilities of the Patriot missile, andthe movement of American warships in the Gulf region. Drones and communicationsystems operated by military personnel are technology-based, meaning any hackof these devices could compromise national security.

According to Thompson(2015), " there are more than seven million devices linked to the Department ofDefense network". With the inclusion of internet, the Department of Defenseplans to increase the number of cybersecurity specialists in the future tosolidify the cyber defenses of the military (NCI, 2015, para. 1). III. Technological Trends " Cryptography has long been used as amethod to protect data. Modern cryptographic techniques are

essential in any ITsystem that needs to store and safeguard personal information” (Hoven, Blaauw, Pieters , 2014). Cryptography isused in information security to protect information from unauthorized oraccidental disclosure while the information is in transit (eitherelectronically or physically) and while information is in storage (Savu, n.

d.). Itspurpose is to practically disguise data so that non-permitted users do not haveaccess. “ The literal meaning for cryptography is ‘ hidden writing’: how to makewhat you write obscure, unintelligible to everyone except whom you want tocommunicate with” (Savu, n. d.). Information and Information technologyhas become increasingly mobile.

Individuals and their devices can be locatedanywhere and move from place to place. “ These devices typically contain a rangeof data-generating sensors, including GPS, movement sensors, and cameras, andmay transmit the resulting data via the Internet” (Hoven, Blaauw, Pieters , 2014, para. 32). Software and data can be saved and transmitted bymeans of email, text, the worldwide web, and social media.

Accordingly, mobilityhas made the task of protecting information more problematic (Denning, 2003p. 9). Mobile software has always posed a major security challenge. Computerviruses, worms, trojan horses, and types of detrimental code have the abilityto enter computers through different forms of communication (Denning, 2003, p. 10).

They account for a substantial amount of all computer security incidentsand can escalate at dangerous rates. IV. GovernmentMany federal

government systems haveinsecurities despite initiatives to consolidate them from foreign attacks(Denning, 2003, p. 12). Following the aftermath of the terrorist attack againstthe World Trade Center and Pentagon, the General Accounting Office (GAO) statedthat “ independent audits continue to identify persistent, significantinformation security vulnerabilities that virtually place all major federalagencies’ operations at high risk of tampering and disruption” (Denning, 2003, p. 12). The personal information of state officials and important civiliancontractors is stored on government owned servers.

The most notable incidentwas in 2015, when the Office of Personnel Management was hacked. A significantamount of its classified information was exposed and put approximately 21. 5million Federal employees at risk of identity theft (Davis, 2015). The attackstargeted not only military information but issues as diverse as freedom ofspeech and critical infrastructure systems operated by multiple private sectorcompanies (NCI, 2015 para. 2). In February 2013, former President, Barack Obama, issued an executive order that read “ Repeated cyber intrusionsinto critical infrastructure demonstrate the need for improved cybersecurity. The cyber threat to critical infrastructure continues to grow and representsone of the most serious national security challenges we must confront. (Staff, 2013, para.

2).” Government organizations need to have the proper knowledge ofthe threats they encounter and improve information security. In a 2012cybersecurity study coproduced with Deloitte, the National Association of StateCIOs (NASCIO) found that 70 percent of state CISOs had reported an

IT securitybreach. In the same study, only 24 percent of state CISOs said they wereconfident about protecting their state's assets from external threats (Staff, 2013, para. 3). (Government Accountability Office, 2014)The graphic above displays thenumber of reported information security incidents involving personallyidentifiable information has more than doubled over the last several years. Majorfederal agencies continue to face challenges in fully implanting all componentsof an agency-wide information security program, which is essential for securingagency systems and the information they contain. In December 2013, GAO reportedon agencies' responses to PII (personally identifiable information) databreaches and discovered they were inconsistent and needed improvement.

V. Large Business/Organization The implementation of an informationsecurity strategic plan can position an organization to diminish, transfer, accept, or avoid information risk related to people, processes and technologies(Evans, 2015). " An established strategy assists an organization appropriatelyto assure the confidentiality, integrity, and availability of information"(2015). Consequently, credit bureau, Equifax, most recently encountered abreach of 143 million Americans' personal information (Sweet, 2017). Thecompany's security team detected suspicious network traffic with the softwarethat ran its online dispute portal. This vulnerability resulted in a loss ofEquifax shares since it announced the breach. No matter how large or small anorganization is, a plan to ensure the security of your information assets isessential (Anonymous). The business benefits of an effective informationsecurity strategic plan are significant and can offer a competitive advantage (Evans2015).

These may include complying with industry standards, avoiding a damagingsecurity incident, sustaining the organization’s reputation and remainingcommitted to shareholders, customers, partners and suppliers (Evans 2015). (Pelisson, 2017) The chart displays the number ofcompromised records in selected large-scale data breaches. The Equifax breachcontained data that is considered most sensitive about individuals includingsocial security numbers, full names, addresses, birth dates, and possiblydriver and credit card information for some (Pelisson, 2017) .

This type of informationis the kind that several organizations such as financial and insurancecompanies use to identify a client accessing their accounts from online, byphone, or in person. Those responsible for the hack, had access to thisinformation between May and July of 2017, and took the company five weeks todisclose the breach (Pelisson, 2017). VI. Answer to Research Question According to Evans (2015), a gapassessment of an organization’s current state and existing efforts is animportant step for security breach prevention. An assessment enables efficientplanning, which then becomes more effective.

Additional steps to building a stablepolicy include defining the vision, mission, strategy, initiatives and tasks tobe accomplished so they enhance the existing program already put in place. AsDenning (2003) stated, the enhanced mobility of technological devices makes itmore difficult for protecting information. It has extended network security’sperimeter from the workplace to homes, airports, hotel rooms, and otherfacilities.

Once information is confined to office networks, it can make way tohome PCs, laptops, computers, and handheld devices which may be less protectedphysically (Denning 2003, p. 9). Each year, tens of thousands of personallaptops are stolen or reported lost, including those that contain secretinformation whether it belong to the federal government, The Department ofDefense, or corporate records (Denning 2003, p. 9). VII.

ConclusionThe importance of InformationTechnology is imperative in the generation of today. Many rely on I. T.

Securityto safeguard vital information from being accessed and stolen. Our nation’sdefense utilizes it in every aspect to counter attack cyber threats that coulddamage national security and compromise military strategies by exposing thelocation of American troops. The Federal Government’s server systems areresponsible for keeping classified information from being stolen by hackers, which potentially poses a threat to national security as well. Big businessesand organizations rely on information security to protect and store data ofcorporate records and clients.

Data such as social security, credit cardinformation, and passwords to communication devices must be protected to avoididentity theft. To prevent these catastrophes from occurring, the government, military, and large business organizations seek assistance from securityprofessionals and analysts. A potential solution to this obstacle is tostrengthen the flaws and gaps located within the organization’s securitymeasures to counter cyber threats that may approach in the future.