Abstract classification model which allows us to

ABSTRACT Informationsystems are frequently exposed to various types of threats which can causedifferent types of damages that might leadto significant financial losses. Information security damages can range fromsmall losses to entire information system destruction. Theeffects of various threats vary considerably: some affect the confidentialityor integrity of data while others affect the availability of a system. Currently, organizations are struggling to understand what the threats to theirinformation assets are and how to obtain the necessary means to combat themwhich continuesto pose a challenge. To improve our understanding of security threats, wepropose a security threat classification model which allows us to study thethreats class impact instead of a threat impact as a threat varies over time. This paper addresses three major threats to information security namely: human, nature and technological factors. These factors are analyzed critically inorder to propose a guideline that helps organizations implement theirinformation security strategies SOURCESOF INFORMATION THREATSintroduction With the development ofInformation and Communication Technologies and increasing accessibility to the Internet, organizations become vulnerable to various types of threats.

In fact, theirinformation becomes exposed to cyber attacks and their resulting damages. Threats come from different sources, like employees, technology and humanfactors. The financial losses caused by security breaches usually cannot preciselybe detected, because a significant number of losses come from smaller-scalesecurity incidents, causing an underestimation of information system securityrisk .

Thus, managers need to know threats that influence their assets andidentify their impact to determine what they need to do to prevent attacks byselecting appropriate countermeasures. Human threatsHuman threats include threats caused by humanactions such as hackers and insiders that cause harm or risk in the systems. Malicious threats consist of inside attacks by disgruntled or maliciousemployees and outside attacks by non-employees just looking to harm and disruptan organization. The most dangerous attackers are usually insiders, because they know many ofthe codes and security measures that are already in place. Insiders are likelyto have specific goals and objectives, and have legitimate access to thesystem.

Employees are the people most familiar with the organization’scomputers and applications, and they are most likely to know what actions mightcause the most damage. Insiders can plant viruses, Trojan horses, or worms, andthey can browse through the file system. The insider attack can affect all components of computer security. Bybrowsing through a system, confidential information could be revealed. Trojanhorses are a threat to both the integrity and confidentiality of information inthe system.

Insider attacks can affect availability by overloading the system’sprocessing or storage capacity, or by causing the system to crash. People often refer to these individuals as “ hackers.” Thedefinition of “ hacker” has changed over the years. A hacker was oncethought of as any individual who enjoyed getting the most out of the system heor she was using.

A hacker would use a system extensively and study it until heor she became proficient in all its nuances. This individual was respected as asource of

information for local computer users, someone referred to as a” guru” or “ wizard.” Now, however, the term hacker refers to people who either break in tosystems for which they have no authorization or intentionally overstep theirbounds on systems for which they do not have legitimate access. The correct term to use for someone who breaks in to systems is a” cracker.

” Common methods for gaining access to a system includepassword cracking, exploiting known security weaknesses, network spoofing, andsocial engineering. Malicious attackers normally will have a specific goal, objective, or motivefor an attack on a system, Philip Sasser (2010). These goals could be todisrupt services and the continuity of business operations by usingdenial-of-service (DoS) attack tools. They might also want to steal informationor even steal hardware such as laptop computers. Hackers can sell informationthat can be useful to competitors. In 1996, a laptop computer was stolen from an employee of Visa Internationalthat contained 314, 000 credit card accounts. The total cost to Visa for justcanceling the numbers and replacing the cards was $6 million.

5Attackers are not the only ones who can harm an organization. The primarythreat to data integrity comes from authorized users who are not aware of theactions they are performing. Cliff Edwards, Olga Kharif, and Michael Riley (2011). Errors andomissions can cause valuable data to be lost, damaged, or altered . Users whoopen up Microsoft Word documents using Notepad, edit the documents, and thensave them could cause serious damage to the information stored on the document. Users, data entry clerks, system operators, and programmersfrequently make unintentional errors that contribute to security problems, directly and indirectly. Sometimes the

error is the threat, such as a dataentry error or a programming error that crashes a system.

Technological threatsTechnological threats are caused by physical and chemicalprocesses on material/ physical processes include the use of physical means togain entry into restricted areas such as buildings, compound rooms or any otherdesignated area like theft or damage of hardware and software. Perrow, Charles (2008). However, chemical processes includehardware and software technologies. It also includes indirect system supportequipment like power suppliesNatural disasters Forces of nature aredangerous because they are unexpected and come with very little warning. Naturaldisasters include fire, earthquakes, hurricanes and accidents which can destroycomputer hardware in a company thus tampering with the system. According toMountain{2016}, they disrupt lives of individuals but also causes damage toinformation that is stored within computers.

These threats can be avoided but the management must have the necessaryprecautions. ReferencesCliff Edwards, Olga Kharif, and MichaelRiley (2011). Human Errors Fuel Hacking as Test Shows Nothing Stops IdiocyIron Mountain. (2016). Protecting vital business from natural disasters.

Retrieved fromhttp://www. ironmountain. com/Knowledge-Center/Reference-Library/View-by-Document-Type/General-Articles/P/Protecting-Vital-Business-Data-from-Natural-Calamities.

aspxPerrow, Charles (2008). Software failure, security and Cyber attack.

Philip Sasser (2010). Human Error and Information Security

Intellectualproperty