A CBSM Framework for requirement-based Proactive Security Measure in Hospitals

TREO Talk Paper

Shounak Pal
NIIT University
shounak.pal@niituniversity.in

Arunabha Mukhopadhyay
IIM Lucknow
arunabha@iiml.ac.in

The IBM Cyber Security Intelligence Report 2017 indicates that the United States (U.S.) suffers an average loss of $225 per data breach which is the highest among 15 countries. The same report also reported that healthcare industry reports a much higher than average loss of $380 per data breach. The price of each patient data can be as high as $363 (Ponemon Report 2015). Recent ransomware attacks on Brookside ENT Michigan resulted in closing of a business by practitioners. Several other attacks on hospitals in Minnesota are also aimed towards demanding ransom in exchange for passwords to unlock patient data (Star Tribune 2019). Healthcare cyber security experts are continuously seeking answers to challenges related to cloud security, unsecured mobile devices, ransomware, IoT devices and people unawareness (HealthcareITNews 2019). Several cyber security provider companies such as Critical Insight (CI) Security have raised funds as high as $9.6 million to expand their analytical ability and reach.

Under the present scenario that includes bigger exploits for hackers and larger investments by security providers and organizations, cyber experts and researchers are stressing on proactive measures such as: (i) investing on evidence-based security implementation and (ii) evaluating security investment. For the purpose, we propose a Classification-Based Security Modification (CBSM) framework which predicts change in each of the security measure’s activity status. We used multiple classifiers like Decision Tree, Naive Bayes and RandomForest to compare and report the classifier that gives us the best result. Our work aims to determine the best combinations among anti-virus (AV), intrusion detection system (IDS) or user authentication (UA) system. It should be noted that most of the present security systems still owe their basic functionalities to the above three systems which cover the requirements for confidentiality, integrity and non-repudiation (C-I-A-NR).

The proposed framework considers routine activity theory (RAT) that explains the use of socio-economic factors within a region that may expose organizations to individual’s tendency to indulge in criminal activity. Our work contributes to the fundamentals of resource-based view it will help the management to determine security changes to ensure sustained competitive advantage. The data for this paper is obtained from three different data sources: U.S. hospital data from (i) Dorenfest Institute for Health Information ( HIMSS) (HIMSS 2004), (ii) Hospital Compare Website maintained by the Centers for Medicare & Medicaid Services (CMS) and state-level data from (iii) America’s Health Rankings (AHR). Our output data, that is, AV_Change, IDS_Change and UV_Change are categorical classes that expresses “if there is any change in their active status compared to the previous year.” On the other hand, our set of predictors are continuous (such as STD_CAS_Change, STD_AAS_Change, STD_HAMR_Change) or categorical (such as Clusters, OwnerType and HospType).

We cluster hospitals into homogeneous sets using hospital characteristics (number of beds) and locational economic condition (literacy, income disparity and per-capita income). The determination for year y is based on standardized value of changes for clinical and administrative automation system (CAS and AAS) and heart attack mortality rate (HAMR) from year (y-2) and (y-1). Accordingly, the general mathematical expression can be shown as,

\[ P_{\text{Security Change}} (CBSM = \{0=No change, 1=Change\} \mid PR_k = \{\text{Cluster}_a, \text{HospType}_b, \text{OwnerType}_c, \text{STD_CAS}_\text{Change}_d, \text{STD_AAS}_\text{Change}_e, \text{STD_HAMR}_\text{Change}_f\} = \frac{(P(CBSM)\cap P(PR_k) | CBSM)}{P(PR)} \]

We observe that Naive Bayes classification technique gives a much better accuracy of 74% than Decision Tree or RandomForest. Our work thus contributes to future research on security investment policy based on hospital performance and motivates managers to proactively improve their security settings based on new technology installations and change in hospital performance.