# Technical brief on cyber security

ASSIGN BUSTER

# Introduction

One of the most challenging components of cybersecurity is the continually evolving world of undertrained staff. The conventional way has been to concentrate resources on essential structure elements and defend against the most significant known threats, which meant giving components undefended and not protecting systems against less harmful risks, such as human error. To deal with the new situation, advisory organizations are encouraging a more effective and adaptive way. The National Association of Standards and Technology (NIST), for instance, recently released updated guidelines in its risk assessment model that suggest The move toward constant monitoring and real-time assessments (Woods, D., Jan. 2018). In the given case scenario, an instructor of a well-established institution has promised to have students' final test scores stored on the lecture building door for all students who anticipate them. The issue with this scenario is that instead of the instructor taking necessary precautions to protect the student's data and other information relevant to the course, they have exposed valuable information to the public. This scenario is perilous because the students could lose their privacy and personal information. Also, the teacher may not be able to provide any protection against misuse of the information that was exposed for a brief period of time. Though the professor's action might've seemed harmless in their sight by exposing sensitive PII, the professor generated a vulnerability that could lead to the impact of a sabotage attack or theft on the student's personal information.

Analysis

a. One straightforward approach in identifying an actor of this caliber that shows no type of malicious intent is to consider their characteristics. For instance, in recognizing the type of category the professor would fall into, I considered the traits of someone who does not follow policy. They will ideally not have malicious traits (though not necessarily) but can create major security concerns due to their lack of awareness and gaps within the cyber framework which leads to unintentional cognitive human errors. As such, it is important to identify the characteristics of a potential attacker before attempting to exploit them and then to identify the vulnerabilities that are likely to be present in a particular situation.

b. Data breaches are becoming an increasing epidemic and taking place almost daily (Silver, C., Jun. 2017). Be though, as it may professionals have an obligation to protect themselves and the clients they serve to the best of their capabilities, or, in this case, the professor had an obligation of due diligence to protect their students (Greenbaum, K., Jun. 2018). Confidentiality, privacy, integrity, data protection and security compliance with the law of the state are a few of the many ethical and legal factors that must be considered when working in the educational domain. Considering universities maintains students personally identifiable information, HIPPA information (this is usually for the medical universities[ex. Phobe]), demographic data, in various cases parental information, grades, disciplinary information, academic performance, and financial information (includes grants, scholarships, Pell) remaining compliant and cohesive to the CIA triad is imperative to the success of the university or any other business that handles the data of the public (Kim & Solomon, 2016). From an ethical standpoint, risk management should be considered to ensure that the information collected by these institutions is not used against individuals or organizations. To enforce legal and ethical factors, substantial policies and boundaries need to be enforced. This includes a strong anti-cybercrime policy, a comprehensive cybersecurity program for all schools and colleges, the use of a secure network, a system of electronic communication systems that can be accessed remotely through the internet and finally, a set of standards for the protection of personal information. A good example of how to implement a strong cybersecurity policy is the national defense authorization act, which requires the federal government to provide funding for cybersecurity programs ( Britannica). The bill also guides how to protect the nation's critical infrastructure from cyberattacks. However, with the given institution in my scenario, a more secure strategy in enforcing policies and boundaries would be to focus on the importance of having a strong cybersecurity policy. The first step in creating a strong cybersecurity policy is to have an understanding of what cybersecurity means. It is important to understand that cybersecurity is not just about protecting your computer or network against intruders. It is also about ensuring that your organization has the necessary resources to protect its information and data. Therefore, when contending with boundaries and policies, it is good to understand that boundaries are helpful in security control because it gives protection through monitoring and controlling systems to counteract and expose malicious and unauthorize access (Fricke, 2018). Boundaries in cybersecurity can also play a vital role in the structuring of an organization's risk management framework (RMF). Additionally, once boundaries are clearly defined, then the framework of policies can begin to be created since the relationship between boundaries and policy are homogeneous. Legally and ethically enforcing protocols can strengthen the compliance of the CIA triad ensuring that organizations execute due diligence to the best of their abilities.

c. Considering the professors didn’t see anything harmful about using a generic report to display their student's final test scores along with other highly sensitive information, this indicates that the professors are not adequately trained to put forth the best cyber literacy approaches. In this instance, one way to respond to this incident is by placing a heavy emphasis on the current state of the data; in this case, it would’ve been in motion when retrieving the data for printing the generic report. If the data-in-motion was encrypted this layer the confidentiality sector of the triad ( Britannica). Additionally, applying the principles of encapsulation and complete mediation in concert guarantees the data will only be visible and read by the intended receiver (student’s). To counter this threat actor, it is recommended that some cyber literacy training be taken. The oblivious actions are another indicator that there is no awareness of how to protect data against unauthorized users rather the data properly is available virtually or through hard copy, the principles of layering and information hiding still apply.

d. The principles of least privilege should be analyzed and considered as a reactive measure to the impact created by the professor. Applying the principles of least privileges will allow for more effective protection of the data considering it authorizes minimal privilege to designated entities to complete their task (Rouse, 2017). In this given scenario, if the least privileges were initially applied the professor would have been able to execute the grading report while limiting the data they have the access granted. Additionally, when the report was generated considering a professor is in an administrative department, he would likely only be able to retrieve student's grades and their identification numbers and nothing more. The social security numbers, home address, and email addresses would've been something that was not available to be accessed by anyone else excluding the human resource department or in this case, the registrar office or office of admissions. Access to this level is better known as role-based access control. For the professor to access this information, they must first obtain permission from the school's administrator. Role-based access control (RBAC) is a necessity because it helps define who your systems or data users are, the role they are in, and what rights is essential for them to have to perform their everyday task without overextending their user's privileges (Bi, M., 2003). Additionally, considering the information that was exposed can't be unseen, I believe it will be necessary for the university to take reasonable precautionary measures given the account. Therefore, the professor should alert the university dean of the incident and the university should contact the students whose information was compromised and offer to help resolve the issue. One way of doing so would be the university offering credit monitoring and alert service to the students. Additionally, they should have a plan of reaction in place in the event some of the student's information does begin being misused to help accommodate the student's damages. Least privilege is the cornerstone IT security concept that refers to limiting access rights for users, reports, and technology operations to the minimum amount required to execute authorized actions (Fischer, E. A., 2014). When effectively applied, least privilege will vastly reduce organizational risk, alter individual productivity, improve systems stability, and change and sustain compliance initiatives. In preparation, least privilege will be difficult to effectively use, particularly when accounting for heterogeneous systems (Windows, Mac, OS, Linux, etc. ), and other cases of users (both inside and vendor).

## Ramification

Considering the damages of having an illiterate cyber aware culture, it is common for organizations to contemplate financial ramifications. If there is no damage assessment considered after the breach of data caused by university professors, then the unintentional behavior will lead to financial losses. These include expenses associated with the incident(s), research and remediation, along with functional disruption. Nevertheless, some organizations remain unaware of the less apparent costs associated with cyber-attacks, which are much intangible, difficult to quantify and under-reported ramifications (Morris, D. Z., Jan. 2016). Additionally, though the principles of least privileges can help provide an acceptable amount of control over who is authorized for a specific level of data; this is only a single layer of defense and though there are restrictions this could cause employees to become vulnerable to phishing attacks to gain entry to the data they are seeking. Though phishing isn’t relevant to other cyber-attacks that seeks to thieve for monetary gain the approach is to steal as much information as possible creating broken trust with customers, the public, and shareholders, loss of finances (to compensate for those impacted and to repair damages) and even release of confidential, top-secret information. For this reason, it is important for the university or any organization for that matter to have a holistic and robust cyber safety policy and scheme in place to provide as much mitigation as possible considering the likelihood of fail secure projects failing as a proactive strategy. Investing in the best tools, implementing the most thought out control, and exercising the best training there is can give the return of helping people realize their obligations to keep their networks secure.

# References

- Woods, D. (Jan. 2018). Why Prediction Should Be Added To The NIST Cybersecurity Framework. *Forbes* . Retrieved from https://www. forbes. com/sites/danwoods/2018/01/18/why-prediction-should-be-added-to-the-nist-cybersecurity-framework/
- Silver, C. (Jun. 2017). Egnyte Protect Helps Prevent Your Company From Getting Pwned By Data Breaches. *Forbes* . Retrieved from https://www. forbes. com/sites/curtissilver/2017/06/28/egnyte-protect-helps-prevent-your-company-from-getting-pwned-by-data-breaches/
- Greenbaum, K. (Jun. 2018). Executive Search And Data Privacy: Four Questions Clients And Candidates Should Ask. *Forbes* . Retrieved from https://www. forbes. com/sites/forbeshumanresourcescouncil/2018/06/11/executive-search-and-data-privacy-four-questions-clients-and-candidates-should-ask/
- (Jul. 2018). National Defense Education Act. *Britannica* . Retrieved from www. britannica. com/topic/National-Defense-Education-Act
- Fricke, J. (2018, September 6). Cybersecurity Architecture, Part 2: System Boundary and Boundary Protection. Retrieved January 16, 2020, from https://insights. sei. cmu.

edu/insider-threat/2018/09/cybersecurity-architecture-part-2-system-boundary-and-boundary-protection. html

- Rouse, M. (2017, November 30). Principle of Least Privilege (POLP). Retrieved from https://searchsecurity. techtarget. com/definition/principle-of-least-privilege-POLP
- (Jul. 2018). Data Encryption Standard. *Britannica* . Retrieved from www. britannica. com/topic/Data-Encryption-Standard
- Bi, M. (2003). Role based Access Control Model. *Computer Science* .
- Morris, D. Z. (Jan. 2016). Railroad Association Denies Smart Train Cyber Vulnerabilities. *Fortune* . Retrieved fromhttp://fortune. com/2016/01/22/railroad-association-denies-smart-train-cyber-vulnerabilities/
- Fischer, E. A. (2014). Cybersecurity Issues and Challenges: In Brief.