Indian Journal of Forensic Medicine and Pathology
Volume 14 Number 2, April - June 2021 (Special Issue)
DOI: http://dx.doi.org/10.21088/ijfmp.0974.3383.14221.40

CASE REPORT

Data Breaches in Academic Enterprise Resource Planning: The Rise of New White-Collar Crimes

Manjeet Kumar[1], Avadhesh Kumar [2], Adarsh Garg[3]

ABSTRACT

Enterprise Resource Planning (ERP) systems are widely used by the academia, and educational institutions. ERP are used by institutions for maintaining their records and sharing of data with the users and stakeholders. ERP modules have varying levels of end-user access restrictions depending on the type of module. Certain modules can be accessed from anywhere using an internet connection, whereas some are restricted to be accessed only through an admin account. These modules generally contain sensitive data stored in them. There are cases wherein the security breach has been reported for gaining access to the data stored and use them for perpetrating crimes, majorly financial crimes and identity thefts. The current paper discusses some of these breaches, along with the possible risks and corrective measures suggested to avoid such breaches.

KEYWORDS | erp, educational-erp, case study, data breach, hei, cyberattack

Authors' Affiliations:
[1]*Research Scholar, School of Business,*
[2]*Professor, School of Computing Science and Engineering, Galgotias University, Greater Noida 201310, Uttar Pradesh, India.*
[3]*Professor, GL Bajaj Institute of Management & Research, Greater Noida 201310, Uttar Pradesh, India.*

Corresponding Author:
Manjeet Kumar

Email: *manjeet.kumar@galgotiasuniversity.edu.in*

INTRODUCTION

ERP is a computer software used to combine all business-related procedures and functions at a combined IT platform for easy management of businesses to work in an efficient way.

ERP is an old technology in manufacturing and production industry that dates back to the early 1960s when the ERP was in the form of Inventory Control system where it acted as accounting software. Later, in the 1970s, this was modified into MRP - Material Requirements Planning, a package that provided support to the planning and control unit of the business houses. This system was replaced by more advanced MRP II system in the 1980s. This new advanced system aims at integration of technology with the manufacturing to increase the manufacturing of products.[1,2]

In businesses, ERP systems keep track of their resources such as raw materials, finance, production capacity, and the standing of business assurances like salaries, sale-purchase orders, etc. This system makes sure that the relevant data is shared with the associated departments of the business and links them together with the core data. In other words, ERP not only ensures the data flow amongst the various departments of the business but also manages the information sharing with the stakeholders of the said business.[6]

ERP in the educational sector is an application that joins all the modules and departments of an educational institution into a single system whose access is available to the fraternity members of the institution and also to the students, their parents, and other stakeholders.[9] Each individual who is part of the institution has a unique user id and password. All the activities can further be monitored by the said administration with the usage of

How to cite this article
Manjeet Kumar, Data Breaches in Academic Enterprise Resource Planning: The Rise of New White-Collar Crimes. Indian J Forensic Med Pathol. 2021;14(2 Special):295-300.

master id and password access. The educational ERP structure is entirely different from that of the business sector [10]. It comprises programs, fees, library, events, hostel, faculty data, examination, which is shown in Figure 1.

Main aim of the educational ERP system is to provide a platform that encompasses all the functionalities together at a user-friendly interface. The educational ERP system digitizes all the information and data of the institute which are updated by admin login only and grants access to all the students and faculties.[11] Educational ERP reduces the need for maintaining the data on paper and keeping a check on the store for ensuring data security. The digitized details once entered into the system are stored on the server which can be accessed only with valid login credentials.[13]

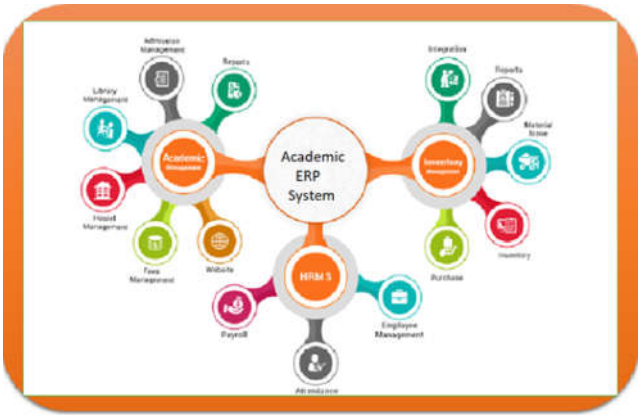

Figure 1: Modules in Academic ERP System

It has been observed by the authors that despite the rise in the implementation of ERP in the educational sector, it can be deduced that 60 to 65 percent of ERP systems have a failure rate and 30 to 35 percent of ERP implementations are canceled because of different factors. There can be numerous factors responsible for this rate of failure, the end-user training, cost input, data security, step-wise implementation rather than the big-bang approach, and lastly the technical training of the users.[14]

For any educational institution, the data of its students is the most valuable asset. With the rise in the technology, the academic institutions are making a change in how they store and process such data available to them, with majority of them shifting to the ERP system for the same. With this shift the concern regarding safeguarding this data becomes a top priority. The threat level has recently increased due to the rise in the cyberattacks, especially during the Covid-19 pandemic times. Another contributing factor in making the data vulnerable is the slow reaction of educational institutions towards cyber security.[15] It has been observed that the academic institutions invest less in cybersecurity making themselves prime targets of cyberattacks. The suggested approach is to make these organizations aware of the security-related issues and build necessary infrastructure.[16]

The survey gives a detailed view of the seriousness of the issue. The security breaches include unlawful disclosures, hacking attempts resulting in the breach of personnel data, ransomware attack, phishing attack, DOS attacks, and other cybersecurity threats, which results in disruptions of academic institutional activities resulting in unauthorized access or disclosure. In the year 2019, 348 incidents were reported related to cyberattacks associated with academic institutions, which is approximately thrice as much as in 2018 in the country of US alone. In 2020, this figure rose further to 377 and will continue to climb as establishments look to get cybersecurity under control. It has been observed that educational institutes are the no.2 target for ransomware attack. [17]

Another associated risk factor is 42% of educational organizations have students or staff as end-users who avoid cyber security protection. For academic organizations, it's compulsory to ensure that they are implementing the appropriate technology to protect themselves from cyberattacks, making sure that they are providing the necessary resources to their users and applying the needed restrictions using firewall to ensure unauthorised access to their network. Another study suggests that 41 percent of higher educational institutions cyber security incidents and breaches were results of social engineering attacks. It has been pointed out that 52% of cyberattack incidents resulting in the data breaches were caused by human error making it the top most cause of such attacks. The act of social engineering revolves around manipulation of its victims in sharing confidential personal information with another individual or third

party. To achieve this, the perpetrator most often impersonate as trusted friend or a colleague of an organization associated with the victim. Another approach employed in social engineering, is the usage of a phishing attack, that is done majorly via emails. It has been observed that an average of 30 percent of users in the academic sectors have been fallen prey of phishing emails received by them. In order to protect its users from such attacks, educational organizations should promote cyber security awareness trainings, ensuring to educate them on related topics of spotting a phishing attack, how to deal with such encounters appropriately when situation arises. [18]

Another survey indicates that 87 percent of educational institutions have encountered cyberattack at least once. These stats indicate that the majority of educational institutions have been the victims of cyberattacks, which is in consistence with the steep rise of attacks reported over the last couple of years. This should serve as a warning to educational administrators to ensure the updating of the cyber security protocols adopted by them. Amongst these organizations, 73 percent are found to be unprepared for cyberattacks, if encountered today.[19] This indicates that the educational institutes must employ the necessary means of technology needed to avoid any such future attacks before a breach occurs. Another study indicates that 85 percent of universities agreed that more investment should be made in order to ensure cybersecurity to protect critical research in IP. In the US alone, the academic sector in 2017, accounted for 13 percent of all data security breaches, which has resulted in the leak of approximate 32 million personnel records. These stats clearly indicate the need to understand the seriousness of cyber security in educational sector. Because of the education industry's approach to cyber security and the end users operating on campus, educational institutions are susceptible to cyberattacks. During the survey, it has been observed that, the educational sector as an industry is the least secured and most vulnerable industry amongst 17 industries studied when it comes to cyber security attacks, when the factors related to application security, endpoint security, and keeping software up to date on a regular basis is considered.[20]

Device standardization that is so common in business that it is much harder to achieve in an educational setting establishments should look to enforce their device management policies and authentication protocols for connected devices as strictly as possible. Awareness training should also be encouraged so that end users are prepared if and when they are targeted by a social engineering attack so they don't cause a breach that compromises the entire institution. According to BlueVoyant's Cyber security in Higher Education 2021 report, ransomware attacks on colleges increased 100% between 2019 and 2020. The report also found that two-thirds of assessed colleges lacked even basic email security measures and 86% of them demonstrated evidence of botnet targeting.

RESULT AND DISCUSSION

Majority of data breaches that struck the educational organizations involved the leaking of the personal information of the personnel and students, whereas about a quarter of the incident reported the exposure of their intellectual property and research work. In an attack on any educational institute the potential risks of data stealing can be related to:

- Complete access to the academic data of students viz, examination scores, overall results which can be changed or deleted.
- Administration can lose important information related to fees and the remaining balance which will result in huge monetary loss of the organization.
- Attackers may intrude in the institute management system and send spam emails or messages demanding confidential information and/or money.
- The biggest threat can be stealing and usage of sensitive personnel information viz, name, address, and age, for perpetuating heinous criminal activities such as blackmailing, loan applications amongst others financial scams. [21]

Any educational institute has numerous challenges which must be dealt to ensure protecting its information and data available with it. Some of such challenges includes:

- The educational sector completely relies on free-exchange of data and information

amongst the involved parties.

- Students and staff members are generally naïve about the technological development.
- Students who have superior technological skills can sometimes attempt cyberattacks out of curiosity.
- Users generally have been assigned more than one role within an organization which creates complications with the identity management software.
- The number of end-users is changed every year with the graduating students leaving and new enrollments coming in.
- In order to ensure smooth access by the end-users it is required to provide remote access of the system so that the parents and their wards can access the system from their personal computers and smartphones from varied locations.[22]

In a survey-based research conducted by Ed Guards Company, disclosed that the incidents related to data breach resulting from cybercrimes dates back to 2002 in US. According to this research in June of 2005, University of Hawaii, witnessed leak of personal data of approximately 150,000 students, staff and library when a former librarian compromised the integrity of the data in order to obtain fraudulent loans. A similar case was encountered at the University of Utah where the social-security number of approximately 100,000 employees was stolen from archived database. Another breach was reported in the year 2006 at UCLA, US, where the cyberattacks precisely aimed at gaining access to personal information, resulting in the leak of approximately 800,000 personnel information including student applicants, their parents, faculty and staff members.[23]

PeopleSoft a system developed by Oracle, which is most commonly adopted by the educational organizations in various countries. The first an foremost attack on this system occurred in the year 2007 wherein hackers by employing keylogger software on staff computers, had stolen the passwords and then used the same to log into ERP system of Florida, A&M University, with motive to change grades of students. Although, subsequently the information stolen was recovered later on, but troublemakers again attempted the similar attack and due to this the examination data of ninety students was modified. In 2008, another attempt was made to access the personal data. Nevertheless, the size of data breached increased from 70,000 to 700,000 stolen records.

In 2012, student of the University of Nebraska's notorious attempt compromised the database of the university which led to the leak of personal information of 654,000 students and employees. Along with the personal information the leaked data included the financial account details of 21000 people, too. Similar cyberattacks were reported at the Chadron State College, Peru State College and Wayne State College in the US.

During the years 2014 to 2016, cyber attacks on academic organizations not only increased in number but also became more advanced and aggressive in terms of data breaches. As per the details shared by the ADBI Report (annual data breach investigations) by Verizon, the occurrence of data breaches distressing the functioning of the educational institutions has grown approximately 10 times in US alone. It is also found that till 2017, the amount of reported cyberattacks was 393 which was only 5 in the year of 2012. In the month of march of 2018, more than 300 universities across the world were affected by a massive cyberattack orchestrated 9 hackers of Iranian origin. According to the information received form the investigating officials, 31TB of valued intellectual property and related data was leaked.[24,25,26]

All educational organizations store personal data of all the students and staff members of theirs. Making sure that this data stored is safe and not easily accessible by everyone is of prime importance to any such organization. The HEIs are rapidly experiencing the increased attacks on their databases by hackers on numerous counts. The data breach is attempted not only to gain access to the personal information of individuals but also include the research materials too.[27]

The most common assumption is that the fact data breach is generally associated with an attempted cybercrime, whereas a data breach can be accidental too, for example a member of staff

may lose his/her laptop or external storage device or the same may get stolen, resulting in loss of the data or confidential information. It may happen that the same can the downloaded on to a USB stick unofficially. Often it can be associated with carelessness which might result in accidental release of data by unintentional correspondence to the wrong person via email.[28]

The most common and effective solution to avoid data-breach is usage of encryption to ensure protection the information. By employing encryptions, academic organizations can be assured that only official users with whom encryption key is shared will be permitted to access and read the information/ data and for others it remains unreadable. This is supported by the study conducted by Ponemon Institute in the year 2017 which revealed that the with the usage of encryption the cost of data breached was reduced by US$16 per record. [29,30,31]

Another vital solution is to provide the necessary training to the IT professionals employed by the organization in case of attempted data breaches. Along with this the awareness training should be provided to the non-technical staff and student members in terms of the safe browsing of the data and safeguarding against the others means of the cyberattacks like social engineering and phishing scams. IJFMP

Acknowledgement:
The authors have not declared any acknowledgment
Conflict of Interest:
The authors declare that there is no conflict of interest regarding this review article.
Source of Funding:
The authors declare that there was no funding for review of this article.

REFERENCES

1. **Acharya. V, Jethava. S, Patel. A.** *(2013). Case study of Database security in Campus ERP System. International Journal of Computer Applications (0975 – 8887) Volume 79 – No 15, October 2013*
2. ***Ali Tarhini, Hussain Ammar, Takwa Tarhini, et al.,*** *(2015). Analysis of the critical success factors for enterprise resource planning implementation from stakeholders' perspective: a systematic review. J. International business research. 2015, vol. 8 No. 4.*
3. **Ashwaq Al Qashami, Heba Mohammad,** *(2015). Critical success factors (CSFs) of enterprise resource planning (ERP) system implementation in higher education institutions (HEIs): concepts and literature review. J. Computer science & information technology (CS&IT). 2015, 10.5121/csit.2015.51508.*
4. **Atif Ali Gill, Arfan Shahzad, Subramanium Sri Ramalu** *(Jun-19). An examination of post implementation success determinants of enterprise resource planning: insights from industrial sector of Pakistan. International Journal of Supply Chain Management, 2019 vol 8 no. 3.*
5. **Bambang P.K., Bintoro Togar Mangihuut Simatupang Utomo Sarjono Putro Pri Hermawan** *(2015). Actors' interaction in the ERP implementation literature. Business Process Management Journal. 2015, vol 21 issue 2.*
6. **Bhattacharya, T and Chellasamy, P.,** *(2016). An analysis of ERP security issues in ERP implementation process of Indian power distribution companies (Discoms). International Journal of Applied Research 2016; 2(7): 34-38*
7. **Davide Aloini, Riccardo Dulmin, Valeria Mininnno** *(2007). Risk management in ERP project introduction: review of the literature. J. Information and management, 2007 vol 44 pp 547 -567.*
8. **Divya Tuteja.** *(2014). Implementation and updation of ERP systems in India: A survey. International Journal For Advance Research In Engineering And Technology. 2014, vol 2 issue III*
9. **Emad Abu-Shanab, Rasha Abu-Shehab, Mousa Khairallah.** *(2015). Critical success factors for ERP implementation: the case of Jordan. International Arab Journal of e-technology. 2015, vol 4 no 1 January.*
10. **Goel, et.al.** *(2012). "Vulnerability Management for an Enterprise Resource Planning System." arXiv preprint arXiv: 1209.6484 (2012).*
11. **Habadi, A., et.al.** *(2017). An Introduction to ERP Systems: Architecture, Implementation and Impacts. International Journal of Computer Applications (0975 – 8887) Volume 167 – No.9, June 2017*
12. **Hamzah Altamony, Dr Ali Tarhini, Dr Zahran Al-Salti, Ala'a Hamdi Gharaibeh, Dr Tariq Elyas.** *(2016). The relationship between change management strategy and successful enterprise resource planning (ERP) implementations: a theoretical perspective. International Journal of Business Management And Economic Research. 2016. vol 7(4) pp 690-703.*
13. **Hongyi Sun, Wenbin Ni, Rocky Lam.** *(2015). A step-by-step performance assessment and improvement method for ERP implementation: action case studies in chinese companies. Computers in industry (elsevier), 2015.*

REFERENCES

14. **Noaman, A.Y., Ahmed, F.F.,** *(2015). ERP Systems Functionalities in Higher Education. International Conference on Communication, Management and Information Technology (ICCMIT 2015). 1877-0509 © 2015 The Authors. Published by Elsevier B.V doi: 10.1016/j.procs.2015.09.100*
15. **O'Leary, D.E.** *(2000). Enterprise resource planning systems: systems, lifecycle, electronic commerce and risk. Cambridge university press. ISBN 0521791529.*
16. **Polyakov, A.,** *ERP Security. Myths, Problems, Solutions. CTO ERPScan (erpscan.com) (last accessed: 30th Nov. 2018)*
17. **R. Addo-Tenkorang, P. Helo.** *(2011) Enterprise resource planning (ERP): a review literature report. Proceedings of the world congress on engineering and computer science. vol II, October 19-21, 2011*
18. **Raafat Saade Harshjot Nijher.** *(2016). Critical success factors in enterprise resource planning implementation: a review of case studies. Journal of Enterprise Information Management. 2016, vol 29 issue 1.*
19. **Sharafat Bibi, Noman Saleem** *(2009). Proposed Security Framework for ERP Systems. Journal of Independent Studies and Research (JISR) on Computing. Volume 7, Number 1, January 2009*
20. **Wanare, R.S., and Mudiraj, A.R.,** *(2014). Security Issue and their Countermeasures in ERP Implementation. International Journal of Management and Social Sciences Research (IJMSSR) Volume 3, No. 6, June 2014. ISSN: 2319-4421*
21. **Fisher, M. D.** *(2006). Staff Perceptions of an Enterprise Resource Planning System Implementation: A Case Study of Three Australian Universities*
22. **Abugabah, A., & Sanzogni, L.** *(2010). Enterprise resource planning (ERP) system in higher education: A literature review and implications. World Academy of Science, Engineering and Technology, 71*
23. **Rabaa'i, A. A., Bandara, W., & Gable, G.** *(2009). ERP systems in the higher education sector: A descriptive study. Proceedings of the 20th Australasian Conference on Information Systems, 456-470.*
24. **Pollock, N., & Cornford, J.** *(2004). ERP systems and the university as a "unique" organisation. Information Technology & People, 17(1), 31-52.*
25. **Frantz, R.** *(2002). John stuart mill as an anti-intuitionist social reformer. The Journal of Socio-Economics, 31(2), 125-136.*
26. **Zornada, L., & Velkavrh, T. B.** *(2005). Implementing ERP systems in higher education institutions. Information Technology Interfaces, 2005. 27th International Conference on, 307-313.*
27. **Murphy, C.** *(2004). ERP: The once and future king of campus computing. Syllabus-Sunnyvale then Chatsworth-, 17(7), 29-30.*
28. **King, P.** *(2002). The promise and performance of enterprise systems in higher education. EDUCAUSE Quarterly,*
29. **Sabau, G., Munten, M., Bologa, A., Et al.** *(2009). An evaluation framework for higher education ERP systems. WSEAS Transactions on Computers, 8(11), 1790-1799.*
30. **Heiskanen, A., Newman, M., & Similä, J.** *(2000). The social dynamics of software development. Accounting, Management and Information Technologies, 10(1), 1-32. doi:10.1016/S0959-8022(99)00013-2*
31. **Birnbaum, R., & Edelson, P. J.** *(1989). How colleges work: The cybernetics of academic organization and leadership. The Journal of Continuing Higher Education, 37(3), 27-29.*

