THE NEED FOR CYBER THREAT INTELLIGENCE FOR DISTANCE LEARNING PROVIDERS AND ONLINE LEARNING SYSTEMS

I. Bandara[1], C. Balakrishna[1], F. Ioras[2]

[1]Open University (UNITED KINGDOM)
[2]Buckinghamshire New University (UNITED KINGDOM)

Abstract

About 80% of further education and higher education institutes have reported data breach or cyber-attacks in the last 12 months. Phishing attacks are being reported as the most common form of cyber-attacks on the university networks. These phishing attacks may be from a variety of sources and have as a reason to steal a variety of data within higher education institutes. The consequences of these attacks may be severe, and the potential route taken by these attacks is via the online learning platforms.

Online learning systems are faced with a unique challenge as numerous systems (student data, learning content and assessment data, lab resources, research, and IP related data etc) are accessed and managed via the Internet by thousands of users over a variety of networks. As a large distance learning provider, Open University has vast experience of managing online learning systems over the past several years. In this study we aim to investigate the areas of vulnerability within the online learning systems. Then propose a framework of IT security policy and procedures to address the identified threats to a university' systems.

Keywords: Cybersecurity, online learning systems, cyber-attack, IT security policies, Phishing attacks, Online learning platforms.

1 INTRODUCTION

Institutions of higher education face a constant deluge of cyberattacks. The risks posed by cyberattacks extend beyond financial losses. While virtually every major industry faces significant cybersecurity challenges, higher education is particularly vulnerable for a number of key reasons. Universities and colleges house a huge volume of sensitive data, from student social security numbers to valuable intellectual property, that, if stolen or compromised, could cause significant damage far beyond the walls of the academia. Cyberattacks use cutting edge technologies and methods to exploit university systems that are, in some cases, lugubriously outdated and outmatched. More specifically, university IT systems are often characterized by a decentralized and some greater decentralization in large research universities that attackers can easily exploit. Nearly 200 universities in the UK have reportedly been hit with at least 850 distributed denial of service (DDoS) attacks in the current academic year [1]. The UK's universities and colleges are facing a growing threat from DDoS attacks, with reports suggesting that students may be to blame for many of them. The Open University in London has been bombarded by more than 1.1 million malicious email attacks from January 2020 to September 2020 [2]. The data collated revealed that 6,804 messages were blocked due to suspicion of malware and 16,452 phishing emails were detected and blocked. Recent research revealed that spear-phishing attacks are excessively targeting higher educational institutions across the world, with over 3.5 million phishing emails hitting over 1,000 global schools and Universities during four months in year 2020 [3]. Spear phishing is a fraudulent practice that targets specific and well-researched users in an organization to collect their credentials using Social Engineering techniques.

Information technology, advanced with new tools, is widely used to enhance online learning; however, often, it does not adequately address the security problems of online education and testing. The security of online learning systems draws the attention of educators actively involved in online teaching. The current coronavirus pandemic forced universities and colleges to replace classroom education by online education, the use of eLearning technologies expanded exponentially. However, online learning systems (OLS) employ the Internet as a place to obtain all necessary information and knowledge. Unfortunately, the Internet has also become the venue for a new-fangled set of illegal activities, so-called cyber-crime [4]. Organisations that do not adequately protect themselves risk the loss or exposure of personal student and staff data and also commercial, institutional and research data that are valuable to cyber criminals operating domestically and internationally [5]. Data must then be protected in order to maintain confidentiality, integrity and availability. Protecting against data manipulation, fraudulent user

authentication and compromises in confidentiality are important security issues in OLS. Meanwhile, OLS trends are demanding a greater level of interoperability for applications, learning environments and heterogeneous systems.

The purpose of this paper is to provide an overview of the most important cyber security challenges that are relevant to Higher Education systems and future distributed OLS. The main sections will cover: cyber security and education; security threats, detection and protection in distributed OLS; developing a security management model for OLS; and, finally, some conclusions are presented.

2 THREATS

Universities are naturally open environments both physically and academically and it is important they retain that open culture. In the Jisc Cyber security posture survey of 2018, surveyed university information technology and security staff seem to better understand their security position. The results demonstrate that perceptions of cyber-security protection are fairly negative [6]. The results demonstrate that perceptions of cyber-security protection importance are impartially negative. Only 15 per cent of Universities and higher education institutes scored 8 out of 10 on a scale where one means 'Not at all well protected' and 10 means 'Very well protected. The mean score was 5.9. Higher education had the highest rate of ransomware attacks among all industries surveyed recently in the report published by BitSight (a cyber risk management company) [7]. Accordingly, universities are working around the clock to shore up their defences against these steep potential losses.

2.1 Cybersecurity and Higher Education

The Higher Education sector is increasingly exploring the use of information systems and technology to meet the needs and expectations of diverse learners who demand more than just traditional classroom-based experiences. OLS attempt to blend face-to-face elements with e-Learning, Webinars and other online digital content. Building trust and encouraging engagement amongst users of OLS is important because there are opportunities for both synchronous and asynchronous interactions with the system. Synchronous learning occurs in real-time, with all participants interacting at the same time, while asynchronous learning is self-paced and allows participants to engage in the exchange of ideas or information without the dependency of other participants′ involvement at the same time. Universities are susceptible to numerous kinds of data breaches due to the vast amount of data they compile from students, faculty, employees, and other individuals affiliated with the campus. In addition to educational records, universities have on-campus healthcare systems, restaurants, bookstores, conference centres, research labs and more. These are the reasons higher education institutions are so susceptible to cyber-attacks because of the openness of their online communities and openness of their critical research data that will become a natural target for cyber attacks [8]. Almost all universities (87%) have experienced at least one successful cyberattack and over a third of UK universities are blighted by a successful cyberattack each hour [9]. These are not just small-scale events to be brushed aside. Attacks on student data are common, including dissertation materials and exam results but critical research IP is highly vulnerable. Majority of data attacks have experienced critical intellectual property theft and grant holder research data. Consequences range from threats to students' and staff personal information, to IP loss and anti-competitive behaviour.

2.2 How Widespread Remote Work Changes Security

The year 2020 brought quick and decisive digital transformations across industries in response to remote work requirements [10]. During this pandemic situation many higher education institutions effectively turned their networks inside out to allow staff and students to work and access the systems from anywhere. This has accelerated both the ongoing adoption of cloud technologies and the organizational support for hybrid working environments. The operational and architectural pivot to a work-from-anywhere model occurred under extreme time and operational pressures, resulting in significant changes to operations and even network configurations themselves. This has expanded the potential methods that attackers can employ to exploit users. Many universities admit they are struggling to deal with cyber security, particularly when it comes to having the right technology to protect and manage data. Students and staff access resources via their own devices and come and go as they please, with universities maintaining little or no control over these personal devices. Universities are often more open and collaborative than most businesses. University data is shared with academics all over the world and every year, thousands of new students arrive, and thousands leave, creating a tidal wave of data security risks. During this pandemic, phishing attacks becoming more sophisticated and

better targeted towards the education sector. The 'Spear phishing' attacks, are those where specific individuals are targeted with requests for information. For example, around the beginning of term, particularly at the start of the academic year, there has been an increase in student grant fraud. This is when students are sent phishing emails purporting to offer free grants or requesting bank details are updated so that loans can be paid [11]. Phishing, ransomware, Cyber-Physical attacks and cryptojacking are among the top cyber security threats and trends that further education and higher education institutes particularly faces [12].

2.3 Vulnerability within the Online Learning Systems (OLS)

Current OLS supporting collaborative learning does not sufficiently meet essential security requirements [13]. Collaborative learning experiences are normally designed and implemented with pedagogical principles very much in mind, whilst security issues are largely ignored. This may lead to undesirable situations that have a detrimental impact on the learning process and its management, such as students falsifying course assessments, presenting a convincing false identity to others, intrusion upon controlled or private conversations, alteration of date stamps on submitted work, and a tutor gaining access to the personal data of students. Kambourakis et al. [14] propose the use of an approach based upon public key cryptography in all OLS environments. Considering PKI requirements for online distance learning networks and attribute certificates (ACs) can provide the appropriate framework to effectively support authentication and authorization services, offering mutual trust to both learners and service providers. Current OLS attack techniques are combined, resulting in threats that are becoming increasingly complex.

2.3.1 Advanced Persistent Threats (APTs)

The emergence of advanced persistent threats (APTs) is clear proof of the sophistication level professionally organised hackers have achieved [15]. APTs are particularly dangerous for universities, as hackers have ongoing access to sensitive data, especially sensitive intellectual property, such as from university research centres, for economic or political espionage. APTs can be divided into five distinct phases: reconnaissance; initial infection; lateral expansion; subversion and exfiltration; the clean-up. Given the sophistication of the attacks, all 5 phases of APT are relevant from a defence perspective and offer opportunities to detect an attack.

2.3.2 Distributed Denial of Service (DDoS) attack

Security experts often talk about the 'CIA triad' which is Confidentiality, Integrity and Availability. Most breaches are a failure of the 'Confidentiality' and the 'Integrity', but in academia the inability to access data or networks (Availability) due to a cyber-attack, such as a Distributed Denial of Service (DDoS) attack that are designed to take networks offline is a real threat. Students and staff are suspected to be behind many distributed denial-of-service (DDoS) attacks at colleges and universities in the UK [16]. Being unable to access an online resource due to an attack may be just an inconvenience for a specific lecture or tutorial, but if the attack persisted or occurred during Clearing or registrations it could cause severe reputational and financial damage. During 2018, more than 1,000 DDoS attacks were detected against 241 different UK education and research institutions [17]. Due to its simplicity to launch attacks and its impact on the victim, a DDoS attack is considered as the most indefensible cyber-attack today.

2.3.3 Scams and Phishing

The most common and effective attack in the higher education sector during this pandemic is via different types of scams and phishing [16]. It is extremely troubling that an attacker only requires a small percentage of clicks to make financial gains or other interests. In this phishing attacks have a success rate of 30% or higher. There was an increase of 600% coronavirus-related phishing email attacks in 2020 [18]. Phishing attacks gets more sophisticated because using machine learning techniques it is quicker to craft and distribute convincing fake messages in the hopes that recipients will unwittingly compromise their organization or universities' networks and systems. Such attacks enable hackers to steal user logins, IP related data and other types of personal information, as well as gain access to private databases.

2.3.4 Ransomware Attacks

Academia has faced increasingly complex cyber-attacks in the last 12 months when students started their new academic year. According to an alert issued by the National Cyber Security Centre (NCSC) there has been a recent spike in ransomware attacks against UK universities and higher education

institutions [19]. It claimed that, in recent incidents, it has observed remote desktop protocols and unpatched software and hardware being utilized, as well as attackers using phishing emails to deploy ransomware. Attackers have also sabotaged backup devices to make recovery more difficult, encrypted entire virtual servers and used scripting environments to deploy ransomware.

3 SECURITY THREATS, DETECTION AND PROTECTION IN DISTRIBUTED ONLINE LEARNING SYSTEMS

Online learning systems (OLS) share the same characteristics and challenges as other e-services, requiring the sharing and distribution of information. More specifically, they are associated with the accessibility of service via the Internet, the consumption of services by a person via the Internet and the payment for a service by a customer. Universities must put greater emphasis on security risk management, taking into consideration the type and severity of the different threats and vulnerabilities, and recognising the diverse interaction and integration between clients, servers, databases and other components.

3.1 Create a security awareness culture

While technical sophistication is essential in protecting universities against cyberattacks, the tools alone, unsupported by users, are not sufficient [9]. Creating a security awareness culture, where everyone in the organisation is aware of the risk and knows their role in protecting this information, is vital. Although universities need to be open and collaborative, this can go too far, leading students and staff to be too lax about their security processes.

3.1.1 Building digital trust

Higher education system became very different environment to what it was several years ago and is now offering significant student engagement via OLS. Students have an increasing understanding of information systems (IS) and information technology (IT) issues, so overall learning strategies devised by course providers must be intrinsically linked with IS/IT strategies to meet student needs now and in the future. Digital natives and digital immigrants will share high expectations of their OLS, in terms of usability, security and protection of their personal information. Universities in the UK hold significant intellectual property through research and other academic materials, which could be attractive targets for cyber-criminals. Researchers will expect their sensitive work and commercially important information to be securely stored, with no risk of theft or misuse. Institutions should perform a cyber security risk assessment and determine best arrangements for technology, people and processes.

3.1.2 Vulnerabilities in OLS

Phishing attacks and malware were present in the top concerns of security professionals in both Further and Higher Education. Security accidents by staff and students also present amongst the top concerns in OLS. Serious security threats that OLS are vulnerable to include software attacks (viruses, worms, macros, denial of service), espionage, acts of theft (illegal equipment or information) and intellectual property (piracy, copyright, infringement). OLS do have some peculiarities, having a variety of users, multiple applications and information to download and upload. Virtualisation is a widely used and popular strategy in all types of enterprises including those in Higher Education. The system offers significant savings on hardware and management costs, supports the implementation of a green strategy, as well as taking advantage of the move to virtualised desktops. When more users move to virtualised environments, more threats will arise. Higher Education institutions need to remember that hosted virtualised desktops (HVDs) should be viewed in the same way as traditional devices, posing the same threats as any connected device [20].

OLS are vulnerable to a range of security threats:

- **Authentication** – broken authentication and session management; insecure communication.
- **Availability** – denial of service.
- **Confidentiality attacks** – insecure cryptographic storage; insecure direct object reference; information leakage and improper error handling.
- **Integrity attacks** – buffer overflow; cross site request forgery; cross site scripting; failure to restrict URL access; injection flaws; malicious file execution.

A threat is defined as a category of object, person or other entities that presents a danger, such as Trojan horses or phishing. Schemes that involve password-based authentication of users are highly susceptible to phishing attacks, which are becoming more and more sophisticated and require strong preventative and countermeasures [21]. OLS platforms are subjected to typical vulnerabilities that characterize information systems. They include XSS (Cross Site Scripting), SQL code injection in the web page, virus and warms, trojan files, password cracking, and others [22].

3.2 Implement a security awareness culture

Accordingly, a trustworthy model of online proctoring and security management model is vital to help prevent cybersecurity attacks that lead to fraud, breaches of the learning content and assessment data confidentiality and the lab resources integrity, disruptions of OLS operations, IP related data and theft of personally identifiable information.

Security management model (SMM) should be based on the fundamental security concepts of CIA triad (confidentiality, integrity, availability) and other security concepts, such as identification, authentication, authorization, accounting, control, non-repudiation, and auditing of online examination processes [23]. The providers of the virtual learning environment, and the tutors distributing the content, are concerned with delivering a secure learning environment and the safe storage of confidential learner data. The learners themselves make a trust judgement about the learning environment and are interested in the protection of their sensitive personal data. Table 1 describes protection against data manipulation, user authentication and confidentiality as important security issues in OLS.

Table 1: Protection against data manipulation, user authentication and confidentiality

Security Risks	***Protection Measures***
• **ARP cache poisoning and MITM attack** • **Brute force attack** • **Cross-Site Request Forgery (CSRF)** • **Cross Site Scripting (XSS)** • **Denial of Service (DoS)** • **IP spoofing** • **Masquerade** • **Rootkits** • **SQL Injection** • **Session Hijacking** • **Session Prediction** • **Stack-smashing attacks**	• Universities should have a robust incident response process capability that addresses malware incident handling. • Consider implementing user interaction-based protection for highly sensitive operations. • Deploy Firewalls for Sophisticated Application attacks • Develop a Denial of Service Response Plan • Installing firewalls and anti-virus software • Implementing Security Management System (ISMS) • Improving authentication, authorisation, confidentiality, and accountability • Using digital right management and cryptography • Training security professionals and IT staff

3.2.1 Continuous Monitoring and Response to Change the Game

The key metric in effectively dealing with ongoing and recurring attacks is the time it takes to respond. Effective response of a threat first requires detecting the threat, then performing the necessary investigation to scope and understand it and taking the needed actions to remediate the threat. Figure 1 shows the attack timeline and response.

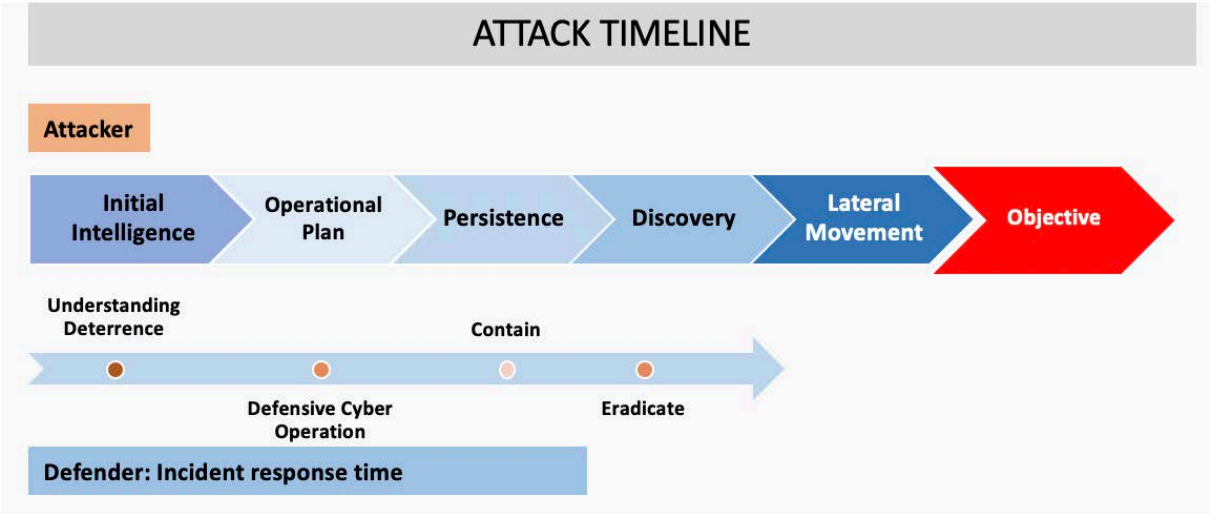

Figure 1: The Incident Response Timeline

4 DEVELOPING A SECURITY MANAGEMENT MODEL FOR ONLINE LEARNING SYSTEMS (OLS)

Universities are now increasingly moving towards cloud computing to deliver applications to students, staff and research teams. Managing security profiles is not easy given the unique nature of universities and achieving the balance of OLS while protecting data is an added challenge. The biggest challenge is ensuring that universities can bridge all of this together, including all of the different security policies and innovations.

4.1 Implementing cyber secure information governance for online learning system

Universities and higher education institutions should implement corporate approaches to managing their information security risks as part of existing governance structures. Institutions have to identify the 'controls' of data in order to establish clear lines of information in institution that shares securely in distributed environment. Security Management Model (SMM) developed will maintain a strong focus on acting quickly to stop a breach, clean up malicious artifacts and help instituitions get back to business quickly. SMM encourages institutions to strive to meet the 1-10-60 rule, where security teams demonstrate the ability to detect threats within the first minute of an intrusion, investigate and understand the threat within 10 minutes, and contain and eradicate the threat within 60 minutes. Implementing cyber SMM need appropriate levels of understanding of the threats facing the university and the measures that have been put in place. It will require day-to-day responsibility for assessing, managing and reporting risks appropriately [20]. While traditional incident response focuses on understanding an attacker's activity and determining root cause, SMM focuses on attack quickly and other artifacts from infected systems and closing holes so the attackers cannot get back in.

4.1.1 The Incident Response Lifecycle

Four main phases of incident response lifecycle are Preparation; Detection and Analysis; Eradication and Recovery, and Post-Event Activity. Figure 2 shows the notion of a "cycle" implies a circular path, where you return to where you were before to continuous monitoring and response process, where new threats are identified and remediated in real time.

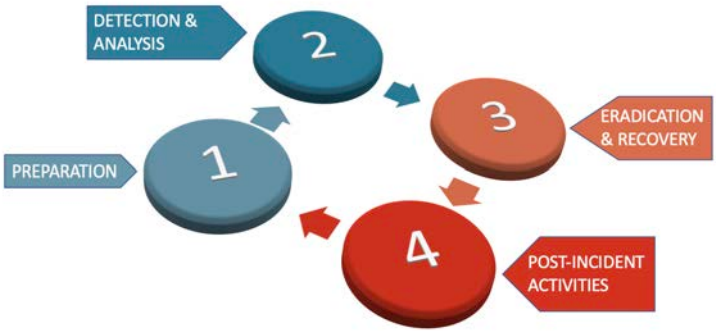

Figure 2: The Incident Response Lifecycle

4.1.2 Security Management Model (SMM)

All the higher education institutions should be aware of their duties regarding the protection of institutional and research data and have appropriate measures in place to ensure that they are compliant with the Data Protection Act (2018) with implementation of the General Data Protection Regulation (GDPR) [24]. Most of the higher education institutions will have different structures for the management of data and research, and appropriate levels of oversight. Most of these institutions and researchers will have variety of data management policies and plans with very little concern on errors. These policies present a challenge for corporate governance to understand both the issues and the necessity of employee cyber security threats process model. The practical use of SMM can be best achieved when there is a culture of working within their institution that best supports cyber-security. This means that the institution's governing body and executive need to provide the leadership that best ensures staff, students and researchers can protect themselves, the institution and their stakeholders from the consequences of accidental information security breaches and cyberattacks. Universities and higher education institutions must demonstrate that their operations and processes are protected [25]. A new British Standard BS31111:2018 has been developed to help governing bodies and executive management better understand the risks associated with IT activities and support decision making that ensures good cyber resilience [26]. Conferring to the SMM, executive management should be capable of providing evidence of the availability of adequate resources (for example financial, human, information, technology) to meet the principles and objectives defined in the cyber risk management and the suitability of the level of preparation and the prevention and response capabilities available to manage a cyber incident.

Looking at cyber-security from a risk management perspective is often familiar for board members who should be used to making risk-based decisions. However, they may not be familiar with cybersecurity or information technology but using the framework provided by BS31111:2018, governing bodies will be able to determine how cyber-security risks are assessed. Network administrators and protectors can maintain up-to-date knowledge of threats and counter measures through exchange of information with peers and with government others. More important is the users which they are crucial to the security of any network and information. They must play a central role in evaluating the risk facing information, security priorities and finally, as users they are responsible for the implementation of controls.

Depending on university or the institution size and culture, individuals may be responsible for a single function or multiple functions; in some cases, multiple people might be assigned to a single function as a team. Figure 3 shows the developed SMM model and high performing security teams understand their individual roles, but also see themselves as a larger team working together to defend against adversaries. The policy and standards team develop, approves, and publishes security policy and standards to guide security decisions within the organization and inspire change. Security architecture translates the organization's requirements and assurance goals into a security vision. Security compliance management is to ensure that the organization is compliant with regulatory requirements and internal policies. People security protects the organization from inadvertent human mistakes and malicious insider actions. The main objective for a data security team is to provide security protections and monitoring for sensitive enterprise data in any format or location. The infrastructure and endpoint security function are responsible for security protection to the, network infrastructure, and user endpoint devices. The main objective of a security team working on identity management, is to provide authentication and authorization of humans, services, devices, and applications. Security threat

intelligence provides context and illegal insights on active attacks and potential threats to empower university leaders and security teams to make better decisions.

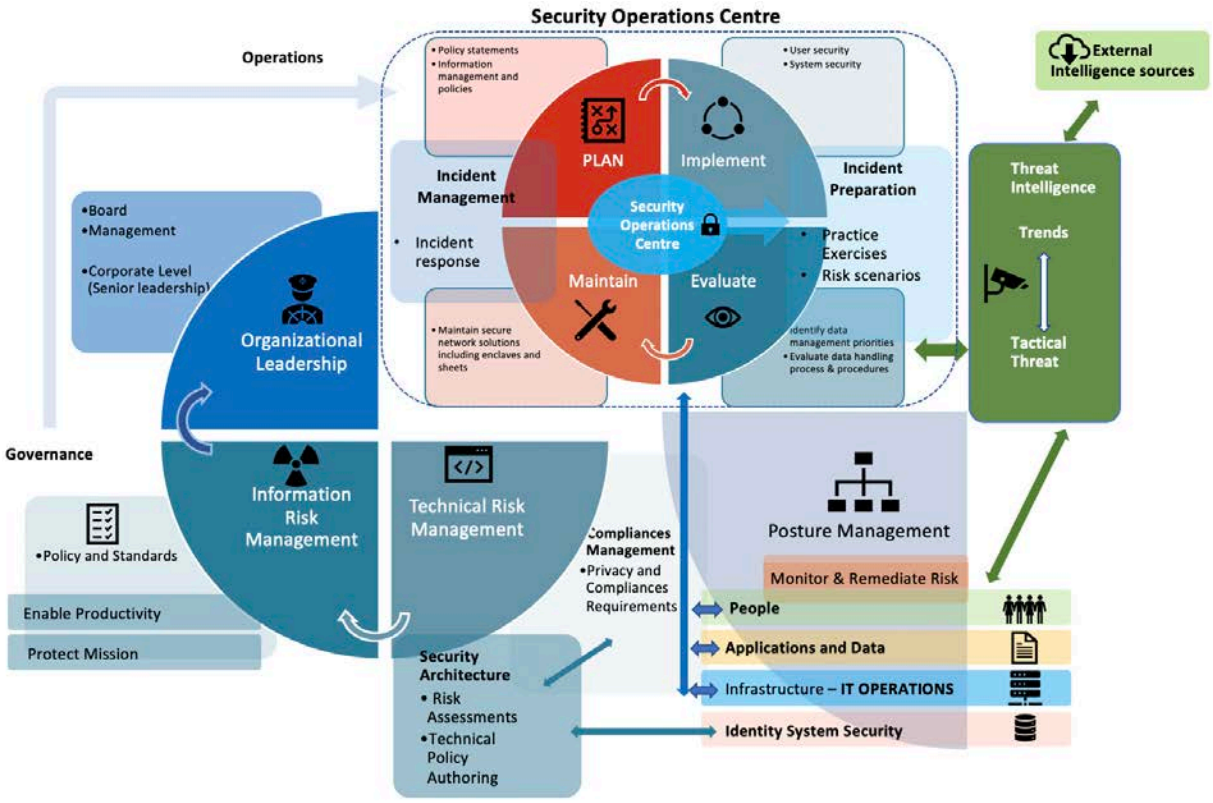

Figure 3: Managing cyber security threats in higher education institutions: security management model (SMM)

5 CONCLUSIONS

As the threat of cyberattacks continues to rise across the higher education sector, the role of the IT department has never been more important in protecting growth and reputation. It is imperative that those in higher education continually assess and improve their security capability and for higher education leaders to take the lead in managing cyber risk to protect students, staff and valuable research data from the growing threat of attack. IT leaders need to collaborate closely with the rest of the university board to ensure protection against hacking, cyber theft and espionage.

This paper also highlights how beneficial a national conversation between those with a vested interest in the protection of universities from cyberattacks is. A number of strategies exist for combating the cyberattacks described above. The increased demand for OLS and their flexibility, mobility and empowerment poses a significant challenge to Higher Education IT departments who are currently finding it harder to maintain control over how data is used, stored and shared inside and outside the virtual class. Understanding users' needs and implementing new services requires building secure, standardised, highly available online learning environments, as well as centralised application management.

REFERENCES

[1] D. Howard Kass., 1st Oct 2018. "DDoS Attacks Target UK Universities: Who's Behind Them" Retrieved from, https://www.msspalert.com/cybersecurity-research/ddos-attacks-uk-universities-jisc-, analysis/#:~:text=Nearly%20200%20universities%20in%20the,in%20the%20current%20academic%20year, 2018.

[2] S. Williams., 12 Nov 2020. "UK university targeted by one million malicious email attacks", Retrieved from https://securitybrief.co.nz/story/uk-university-targeted-by-one-million-malicious-email-attacks, 2020.

[3] Aleroud, A., Abu-Shanab, E., Al-Aiad, A. and Alshboul, Y. “An examination of susceptibility to spear phishing cyber attacks in non-English speaking communities”. Journal of Information Security and Applications, 55, p.102614., 2020

[4] Bandara, I., F. Ioras, and K. Maher. "Cyber security concerns in e-learning education.": 7th International Conference of Education, Research and Innovation, p. 0728-0734, 2014.

[5] H. Johnson. "Dialogue and the Construction of Knowledge in E-Learning: Exploring Students' Perceptions of Their Learning While Using Blackboard's Asynchronous Discussion Board," European journal of open, distance and e-learning, no. ISSN 1027-5207, 2007.

[6] Chapman, J., Chinnaswamy, A. and Garcia-Perez, A. January. “The severity of cyber attacks on education and research institutions: A function of their security posture”. In ICCWS 2018 13th International Conference on Cyber Warfare and Security (p. 111). Academic Conferences and publishing limited, 2018.

[7] J. Alcon., 13 October. “13% Of The Higher Education Sector Has Been Infected With Ransomware”, Retrieved from, https://www.bitsight.com/blog/higher-education-infected-with-ransomware, 2016.

[8] Lallie, Harjinder Singh, et al. "Cyber security in the age of covid-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic." arXiv preprint arXiv:2006.11929, 2020.

[9] VMware. “University Challenge: Cyber Attacks in Higher Education”, Retrieved from, www.vmware.com, 2009.

[10] Shawn Henry., “Crowdstrike Services Cyber Front Lines Report”, Retrieved from, https://go.crowdstrike.com/2021-crowdstrike-services-cyber-front-lines-report.html?utm_campaign=brand&utm_content=neu&utm_medium=sem&utm_source=goog&utm_term=%2Breport%20%2Bcrowdstrike&gclid=CjwKCAiAu8SABhAxEiwAsodSZAy78j71zlEa0voo5hPtZ9MDXA_8EUVrZw2a1sdQmQSAibfUVIXHeBoCDIsQAvD_BwE, 2021.

[11] Stephen Little, “Fake tax refund scam targeting university students reaching unprecedented numbers, warns HMRC”. Retrieved from https://www.ii.co.uk/analysis-commentary/fake-tax-refund-scam-targeting-university-students-reaching-unprecedented-numbers-warns-hmrc-ii512872, 2018.

[12] Coughlan, s. “BBC News family and education correspondent”. Retrieved from, Cyber threat to disrupt start of university term, https://www.bbc.co.uk/news/education-54182398, 2020.

[13] Kambourakis, Georgios, et al. "A PKI approach for deploying modern secure distributed e-learning and m-learning environments." Computers & Education 48.1 (2007): 1-16.

[14] J. M. Moneo, S. Caballe and J. Prieot, "Security in Learning Management Systems," eLearning Papers, Catalonia, Spain, 2012.

[15] Abu, M.S., Selamat, S.R., Ariffin, A. and Yusof, R. “Cyber threat intelligence–issue and challenges. Indonesian Journal of Electrical Engineering and Computer Science”, 10(1), pp.371-379, 2018.

[16] National Cyber Security Centre (NCSC) and Cybersecurity and Infrastructure Security Agency (CISA). Advisory: “COVID-19 exploited by malicious cyber actors”. Retrieved from https://www.ncsc.gov.uk/news/covid-19-exploited-by-cyber-actors-advisory, 2020.

[17] Tomáš Foltýn., “Who's behind DDoS attacks at UK universities?”, Retrieved from https://www.welivesecurity.com/2018/09/28/whos-behind-ddos-attacks-uk-universities/, 2018.

[18] Sjouwerman S. “coronavirus-related phishing email attacks are up 600%”. Retrieved from https://blog.knowbe4.com/q1-2020-coronavirus-related-phishing-email-attacks-are-up-600, 2020.

[19] Dan Raywood. “Universities Face Increase in Ransomware Attacks as Students Return”, Retrieved from https://www.infosecurity-magazine.com/news/universities-ransomware-attacks/, September 2020.

[20] Bandara, I., F. Ioras, and K. Maher. "Cyber security concerns in e-learning education.": 0728-0734, 2014.

[21] S. K. Sood, "Phishing Attacks: A Challenge Ahead," elearning papers, April 2012. Retrieved from, http://www.openeducationeuropa.eu/en/paper/cyber-security-and-education. 2014.

[22] Sharma, Pankaj, Rahul Johari, S. S. Sarma. "Integrated approach to prevent SQL injection attack and reflected cross site scripting attack." International Journal of System Assurance Engineering and Management 3.4, 343-351, 2012.

[23] Chapman, J. “How safe is your data? Cyber-security in higher education”. HEPI Policy Note, 12, pp.1-6, 2019.

[24] Data protection, “The Data Protection Act”, Retrieved from, https://www.gov.uk/data-protection, 2018.

[25] Warwick, A. “Hackers targeting UK universities a threat to national security”, Retrieved from, https://www.computerweekly.com/news/252464169/Hackers-targeting-UK-universities-a-threat-to-national-security, 2019.

[26] BS 31111: “the new cyber security standard explained”, Retrieved from, https://www.itgovernance.co.uk/blog/bs-31111-the-new-cyber-security-standard-explained, 2018.