2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA) | 978-1-7281-8543-9/20/$31.00 ©2020 IEEE | DOI: 10.1109/TPS-ISA50397.2020.00046

Envisioning a Cyber-Security Incident Managed Campus Environment

Sean Thorpe, Julian Jarrett, Tyrone Grandison
Faculty of Engineering and Computing
University of Technology
Kingston, Jamaica
{thorpe.sean; jarrett.julian, tyronewagrandison}@gmail.com

***Abstract* — This vision paper posits the need for a managed cyber-security incident response requirement for the main campus of the University of Technology, Jamaica. Since the COVID-19 pandemic, the institution has pivoted to a significant online offering for the teaching and learning outcomes for its students. The paper provides unique summary perspectives of the cyber-security incident challenges and opportunities within a university operating in a developing country. These concerns are raised to motivate similar educational institutions, as well as small and medium size organizations, during this pandemic.**

Keywords— cyber-security, incident, response, pandemic

I. Introduction

The information security policy for the University of Technology, Jamaica (UTech) requires an urgent revision to address the cyber-security incident response and recovery necessary to support wide scale virtualization initiatives particularly since the COVID-19 pandemic. This is most likely the case in other academic settings. This paper identifies precautionary activities that the university should urgently seek to implement given the pandemic challenges. The role of management in establishing the necessary antecedent to drive cyber security within the university at this time underscores a significant and very urgent need during this pandemic.

UTech, Jamaica is the only national university in Jamaica offering an array of graduate and undergraduate degrees across various disciplines. It obtained its mandate through an act of Parliament - the University of Technology Act of 1999. It has roots in the Jamaica Institute of Technology founded in 1958, which was renamed to the College of Arts, Science and Technology (CAST) in 1959. UTech operates predominantly through its main campus in Papine, Kingston and more recently through various satellite campuses across the cities of Kingston and Montego Bay. The university has implemented blended learning for some programs. However, it does not have a full online offering or a fully operational virtual space for much of its teaching modalities. In the era of the COVID-19 pandemic, UTech and many other businesses and institutions across the world has had to seek virtual alternatives for business continuity; a key critical success factor for the University to meet the needs of its stakeholders. The campus-wide virtualization of computing laboratories has had a major impact on student engagement. Through virtualization, several physical computing laboratory tasks have become automated and provides an overall net savings to the University when solutions are scaled. Classes are provisioned in batches or arranged by students utilizing various instructor-configured environments; consisting of one or more subnets, each containing one or more operating environments, each containing one or more Virtual Machines.

There is also growing evidence of the need for a clear BYOD access control security policy with a restriction on the number of devices that can be connected on the campus network should be guided. Additionally, the need for an updated secure wireless access and use policy guided by some standard form of **encryption (ex. WPA)** is required. Both concerns should comprise of the operations governed by the Information Security Office (ISO).

Finally, the cyber security policy strategy and operation won't be as effective without a comprehensive security awareness programme as a consideration for the significant human element that will need to lead as well as use the Cyber-security policy. At the centre of the security awareness programmes are both staff and students. This means that the ISO through its function has to continuously train and retrain staff and student communities on the importance of the various information systems that it uses including the new ones to be implemented.

II. Challenges

The virtualization of campus area networks must ensure provable end point security at all levels to mitigate or de-risk the likelihood of malware vulnerabilities. The source of such vulnerabilities range from poor design techniques in the local area network (LAN) infrastructure to man-in-the-middle, and denial of service attacks which may go undetected. The source of these threats can be both internal or external to the campus network. The deliberations of the university must be proactive concerning the adoption of guiding sustainable security policies and procedures. The problem becomes exacerbated when the entire campus network becomes virtualized, where the user's digital

DOI 10.1109/TPS-ISA50397.2020.00046

footprint becomes more volatile and difficult to detect and track.

Another independent but related concern is the proliferation of wireless access points distributed across campus; these access points have increased across the university to improve greater connectivity and access for students. Recent increased usage by students and staff via some Bring Your Own Device (BYOD) modality since the pandemic, escalates the sources of possible attack for the campus network, increasing the challenges of incident identification and response. Malware attacks can be launched from a BYOD mobile device connected via an access point to the campus network, presenting a threat vector of 12,000 possible students and another 1000 possible staff members excluding the fact that the campus environment is open to the general public as guest. The odds of finding the attacker becomes increasingly difficult if the suitable network tracing and monitoring technologies are not used by the system administration teams that have remit for the network.

III. OPPORTUNITIES

As a part of the practice of any good Information Technology (IT) Governance, the university has the opportunity to employ a cyber-incident identification and recovery policy, as well as the formal operational procedures, that supports the policy operations given the description of the type of challenges described above. Inherently this alludes to the fact that layering virtualization into the network requires that the enterprise digital architecture of the university include a layered level of security abstracting specific concerns as required.

An effective cyber incident identification, containment, recovery, and follow up, must be consistent with the international guidelines and best practices outlined in the ***National Institute of Standards Technology (NIST) 800-61*** [1] that speaks to the handling of Cyber-security incidents.

Developing a comprehensive policy and operational procedure is a non-trivial consideration that should consider:

I. Mapping the business processes within the University and implementing the digital assets and the priority of these assets in the face of an incident response and recovery requirement.
II. Evaluating the incident response mechanisms that need to be activated based on the priority of the asset classes identified and to ensure they are compliant with the international provisions based on the guidelines in [1].

Customarily in universities, like in any other business, they need to broker special service level agreements to help formulate and guide policy issues relating to a cyber-incident requiring the setup of a special project office called the "***Information Security Office (ISO)***" within an appointed office of the ***Chief Security Officer (CSO)*** and a requisite ***Security Incident Response team (SIRT)*** tasked with oversight of the operations consistent within the university's guidelines. This ISO provision is separate from the traditional disaster and recovery risk mitigation function that is already handled by the Safety and Security department concerning strictly physical security incidents. Arguably, the Safety and Security department embraces the need for digital security within the physical environment. This is evident as they incorporate more Internet of things (IOT) devices across campus. The overt gap with respect to the skills required to handle the IOT incident response supports the argument of the complementary SIRT operation within the ISO. As COVID-19 cases spiked, the university was required to radically shift to a more than 90% online campus. This shift demonstrates the need to ensure an improved digital security experience given the increased footprint of students and staff in cyber-space at this time.

The opportunity cost of not having an ISO is even more expensive and hence a deliberate strategy is urgently required to avoid any further disruption with respect to the university operation. The impact of non-virtualization renders the campus to a state of paralysis or shutdown to support the basic teaching and learning communities. The claim by the general IT department that IT security is an independent operation, further justifies the need for the ISO. The role of the ISO as a managed function of the security governance for the university requires that the appointed Chief Security Officer in the office of the ISO has autonomy to drive policy and operation and reports directly to the university's council, which is the final accountable authority within the university. Considering that the Jamaican legislature is now in the right of passage of its own data protection laws, the ISO is well positioned to ensure that a data protection function is also assigned as a part of the ISO to support the university's data protection enforcement and compliance. The ISO would work towards maintaining a digital asset classification library, where all the faculties, colleges, service units, divisions and departments across the university sensitive data inventory situated across all the various IT systems within the university are tracked. This will aid with incident categorization required as a part of any impact analysis on the various IT systems that risk being compromised in the face of a malware attack.

The proposed University Information Security Office will need to be recognized under the well-established international ***ISO 27001*** *framework* for Information Security (formally known as **ISO**/IEC **27001**:2005); a specification for an information security management system (ISMS). An ISMS is a framework of policies and procedures that includes all legal, physical and technical controls involved in an organization's information risk management processes. Through the efforts of the Jamaica Bureau of Standards Working group ISO 27001 in 2013, Jamaica as an island state that now legally observes the ISO 27001 and that supports the adoption of the intended University ISO operation.

Since the COVID19 pandemic the campus has been actively looking at virtual laboratory solutions [2,3,4]. As the university plans ahead post COVID-19, virtualization security of the platforms and infrastructure will have to be embraced as a part of business continuity. In the model of

the solution for virtualization laboratories used in [4], it has been realized that the infrastructure provides cybersecurity and cyber forensics auditing for its students on a 24/7 online all-the-time environment accessible in the classroom, online anywhere within the campus and the world. The use case of the virtual labs solutions argues well for the need to implement the office of the ISO with even greater urgency, once one has moved all the virtual labs to full production campus wide.

IV. CONCLUSION

This vision paper argued for the need for campus environments in developing countries like UTech, Jamaica to have a managed cyber-security incident response especially since the COVID-19 pandemic where the campus has had to pivot online. These online environments have become increasingly prone to cyber-attacks and are particularly challenged if the enterprise architecture of the campus networks are not adequately equipped to drive the virtual and online platforms during this time.

The Information Security Office (ISO) would autonomously help to drive strategic policy direction and implementation in this regard. The use case also lends itself to other similar developing countries and their educational institutions in these jurisdictions that need to pivot to full virtualization within the online environment. Additionally, small and medium size companies within developing countries may also leverage the views shared for their own contextual adoption given their own circumstances.

Through the ISO for the university, that of a small and medium size enterprise or otherwise will need consensus on the digital asset inventory within their environments requiring a cyber-security incident response. This allows for easier incident identification and response given the digital asset classification libraries that would be created. Furthermore, the managed ISO operation can be used within the campus organization or otherwise to drive ongoing security awareness training programmes that educate on how to protect and manage the user-centric privacy and security of your digital space.

REFERENCES

[1] NIST Computer Security Response Handling Guide- https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

[2] Info security Learning Labs https://www.infoseclearning.com/virtual-labs, retrieved September 30, 2020.

[3] Virtual labs An initiative of the Ministry of Hyman resource Development https://www.infoseclearning.com/virtual-labs, retrieved September 30, 2020

[4] Glen Dardick – Virtual laboratory at Cyber Explorations https://www.cyberexplorations.com/