Information Security on the Curriculum

Physical Red Teaming within the Educational Sector

A Whitepaper from:

Peter Daniel

Security Consultant

Executive Summary

The Educational Sector, and specifically universities, have seen an upsurge in being targeted by cyber threats, with calls for universities to *"acknowledge the risk that they are under"*.[1] Commentators, such as the National Cyber Security Centre (NCSC), have recently issued reports (September 2019) explicitly focused on higher educational institutions, urging both an upskilling of staff awareness, as well as of technical and physical controls.[2] This report was spurred by a publication by the JISC (Joint Information Systems Committee) and the HEPI (Higher Education Policy Institute), in April 2019, documenting a simulated cyber-attack on 50 universities within the UK – all of which were successfully breached within two hours.[3] Combining these results with UK universities now being fined for data breaches by the Information Commissioner's Office (ICO), this should motivate these institutions into seeking advice and guidance on improving their security posture.[4]

Resources, such as penetration testing and Information Technology Health Checks (ITHCs), provide an evaluating means to discover any technical vulnerabilities within an organisation, whereby remediation effort can be invested on additional measures or refining pre-existing controls. Whilst this is in accordance with best practice guidelines, it does not address vulnerabilities inherent within the organisation's physical security. One prominent approach is through Physical Red Teaming exercises, which seek to address this deficiency. Due to an evolving convergence of the technical and physical, accentuated by the Internet of Things (IoT), both assessment methodologies need to be utilised for assurance purposes.

Introduction

Living in a progressively digital age certainly brings about a multitude of benefits, many of which are concerned with an improved sense of productivity, efficiency, and empowerment. Not only does technology aid in knowledge transfer through global connectivity, but also as a form of recreational escapism from the stresses of modern life. Despite so many uses, what is difficult to escape from is its heavy burden of risk, made evident with a plethora of news headlines drawing attention to the latest information security breach. Information, in its widest sense of the word, is increasingly adhering to this digital trend, with personal and account details being stored, shared, and displayed in an electronic format.

As such, and under the ever-watchful gaze of the enhanced powers of the Information Commissioner's Office (ICO), focus has been, understandably, afforded to the technological protection of digitalised information through logical security controls. Whilst this is all well and good, what has fallen by the wayside is the consideration of robust physical security measures to ensure that direct tampering cannot take place:

[1] https://www.infosecurity-magazine.com/opinions/universities-attackers/
[2] https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities
[3] https://www.bbc.co.uk/news/education-47805451
[4] https://www.bbc.co.uk/news/technology-44197118

"You can fortify a server as much as you'd like with logical security measures, but if you leave it out in the middle of an open field, they're not going to do you much good…".[5]

This paper explores this particular premise, especially in reference to the Educational Sector, and aims to explain one methodology by which physical security effectiveness can be adequately measured. Advent IM terms this validation technique as 'Physical Red Teaming', and in accordance with penetration testing and Information Technology Health Checks (ITHCs), this is a means by which physical unauthorised entry is undertaken, in comparison to more illicit logical access attempts.

The Educational Sector as a Target

Universities are a hub of technological developments and scientific research, some of which being of a sensitive nature and of national interest. This makes it somewhat of an attractive commodity to those seeking financial gain through theft of designs and intellectual property, or by disclosing such information to competitive third-parties and even nation states. That's not to mention the vast quantities of staff and student personal information readily churning on an annual basis. If this information is obtained by malicious groups, this can be auctioned and sold on the dark net, or additionally used for further exploitation through phishing schemes and blackmail.

Whilst financial incentives are predominately a reason for waging an assault against any organisation, the Educational Sector may be targeted for the sole purpose of operational disruption, as well as the destruction of valuable records. Threat actors may include protest and activist groups (especially post speculation or leaks of unethical research), state-sponsored or state-coerced individuals or groups (international students may be susceptible to this), or disgruntled employees. Concurrently students themselves, dismayed by the rising costs of tuition, poor results, or suspension/expulsion, may seek to disrupt operations or tamper with/destroy attainment evidence. This may also ring true of relatives whom place blame on the university for a lack of achievement.

One example of an ex-student with malintent is a Vishwanath Akuthota, a 2017 alumnus of The College of St. Rose in Albany, New York, whom was found guilty of vandalising university property using a weaponised 'Universal Serial Bus (USB) Kill Drive'. This particular drive, bought online by Vishwanath, was designed to destroy computer equipment through discharging a high voltage, electrical pulse to fry not only the port, but also other components including the Central Processing Unit (CPU). By using this drive, in 2019 (two years since his graduation), Vishwanath successfully damaged upon repair *"59 Windows workstations and seven iMacs alongside numerous monitors and digital podiums".* [6] This begs the question as to how he was still granted entry into these restricted university spaces with his access rights still remaining active, as well as there not being any physical locking mechanisms on the affected workstations themselves. Moreover, it should highlight wider risks of such drives being inserted into an organisation's server room, as this could immensely disrupt business operations.

Insider threats have yet again been identified as being a key risk factor to cyber security, by continuing to hold a place on top cyber threat predictive lists for 2020.[7] It should be noted and

[5] Some consultant at Advent IM
[6] https://www.infosecurity-magazine.com/infosec/usb-breach-physical-security-1-1-1/
[7] https://builtin.com/cybersecurity/cybersecurity-threats

recognised that this does not make an assumption that all insider threats (namely employees, but in this case includes students) are acting maliciously. Breaches or unintentional information disclosure may be the consequence of mistakes, a lack of wider security awareness, or a lack of adequate training. The National Cyber Security Centre's (NCSC) September 2019 report into the cyber threat to universities markedly states that university institutions may especially find maintaining security awareness difficult due to vast turnovers in both staffing as well as student levels.[8]

Concurrently, the NCSC's report continues to urge that universities must upskill not only the overarching security awareness of both staff and students, but also their technical and physical mitigation controls. This assessment has been based on the publication of research by the JISC (Joint Information Systems Committee) and the HEPI (Higher Education Policy Institute), in April 2019, documenting a simulated cyber-attack on 50 universities within the UK – all of which were successfully breached within two hours.[9]

Understanding the risks posed to an organisation is one of the initial steps required to preparing and deploying a sufficient remediation strategy. As we embark on 2020, and in light of the rise of Internet-connected devices or IoT (Internet of Things), there has been an appetite for the convergence of Cyber and Physical Security.[10] Most notably, architecturally speaking, the result of technological developments have birthed the age of Smart Buildings – those which are constructed with intelligence and automation in mind for system efficiency, operational utilisation, and reductions in energy footprints.[11] Universities are subsequently adhering to this trend by taking full advantage of data capture and analytics to improve the student experience.[12]

Suffice to say, this emerging convergence also presents new risks. The crossover between physical and technological assets has created an inter-reliability which, put simply, means that if one is compromised, the other is brought down with it. A prime example of this is the abundance of news articles and reports of keyless car crime via relay theft, with WhatCar describing how vehicles *"can be stolen far more quickly and easily than those with conventional locks and ignitions"*.[13]

Aided by national interest through media coverage of data leakages/breaches and subsequent financial penalties by the ICO, there has been a principle focus on the technical element of information security – namely through the promotion of the 'Cyber' buzzword. With Cyber at the forefront of headlines and easily digestible content, the physical perspective has arguably slipped into the background.[14] Despite this, to understand the more tangible aspect, an explanation into Physical Security is required.

Physical security is based on the principles of deterrence, delay, and the traditional outlook of reducing the opportunities for criminality to take place. The Centre for the Protection of National Infrastructure (CPNI), the leading authority on physical security, illustrates that effective physical security is achieved through the multi-layering of different control measures – referred to as a

[8] https://www.ncsc.gov.uk/report/the-cyber-threat-to-universities
[9] https://www.bbc.co.uk/news/education-47805451
[10] https://www.securitymagazine.com/articles/90960-preparing-for-physical-and-cybersecurity-convergence
[11] https://www.trueoccupancy.com/blog/what-is-a-smart-building
[12] https://www.jisc.ac.uk/rd/projects/intelligent-campus
[13] https://www.whatcar.com/advice/owning/keyless-car-crime-%E2%80%93-what-are-car-manufacturers-doing-to-prevent-it/n19894
[14] https://www.csoonline.com/article/3504953/physical-security-being-overlooked.html

'defence-in-depth' approach.[15] Each layer should be interdependent, supportive, and means tested to ensure that assets are sufficiently protected from the risk of unauthorised access or modification. Nevertheless, how can an organisation means test such controls? One such method of validation involves performing a Physical Red Teaming exercise…

What is Physical Red Teaming?

Advent IM defines Physical Red Teaming through the following:

"Red Team testing was born out of a requirement to evaluate and test physical and procedural security measures with realistic, Threat Analysis based scenarios".[16]

In effect, this is a pre-authorised, simulated/non-destructive attack against a building or locality in order to gain access, especially where possible, into restricted zones and areas of interest. This is conducted with prior approval from the organisation being tested, with knowledge of the operation being limited to only a select number of people to gauge unprepared responses from their employees. Just think burglary, but the residents are likely to still be at home and nothing is removed from the premises…

Now this is not to be confused with logical red teaming exercises – those of penetration testing scenarios which pit a red team (attacking force) against a blue team (defending force) for breach and control of a network. Physical Red Teaming objectives are to evaluate the effectiveness of the organisation's intrusion detection systems, access controls, and security policies and processes, as well as the overarching security awareness and vigilance of its employees.

Physical Red Teaming exercises utilise an assortment of realistic techniques, such as tailgating, social engineering, and wider reconnaissance to imitate the strategies employed by threat actors.

Benefits of Physical Red Teaming

Conducting a Physical Red Teaming exercise provides the opportunity to objectively examine and validate the effectiveness of an organisation's physical security controls. This is not limited to environmental measures such as intrusion detection and access systems, but also to means tests the adequacy of implemented policies and procedures. It answers the question of whether the company's employees have knowledge of and comprehend the standards in place, and are readily aware and vigilant of any potential threats.

Moreover, such exercises confirm whether additional security awareness training is required to be undertaken by staff, as well as whether pre-existing controls in place need enhancing or amending for heightened effectiveness. For example, testing may establish the need to reposition CCTV cameras for greater visibility and detection rates, or alternatively to quell apprehension

[15] https://www.cpni.gov.uk/physical-security
[16] https://www.advent-im.co.uk/testing/red-teaming/

about a particular entrance route or means of gaining unauthorised access into the target building/restricted area.

Furthermore, Physical Red Teaming scenarios can be tailor-made to replicate realistic scenarios which address an organisation's key risk concern. As mentioned previously, groups such as activists or disgruntled students pose a risk to Universities, so infiltration attempts could be made under this guise.

Personal Experiences of Physical Red Teaming

As the highly esteemed author of this whitepaper and obvious leading authority on everything 'Physical Red Teaming-y', it is worth sharing some thoughts based on my own experiences within the field.[17] Below is a list of some of my own personal reflections*, which may or may not serve as guidance notes:

- **Larger organisations are more susceptible to physical intrusion:**
  Higher staff turnover and higher quantities of footfall accommodate an environment of invisibility. Firms with vast employee numbers make it nigh impossible for people to know every single one of their colleagues, which allows for an assailant to 'hide amongst the crowd'

- **Politeness should not always be lauded:**
  This is in particular reference to the time-honoured, chivalrous tradition of holding doors open for people. Not only does this encourage tailgating, but also makes access controls, such as Radio Frequency Identification (RFID) entry systems, redundant

- **Employees just do not have the time to notice:**
  Excessive workloads and demand for productivity comes at the cost of vigilance. As long as the situation has no direct impact on an individual, there is no personal cause for concern. One fond example of this is where I spent a good five-to-ten minutes pressing random buttons on a corporate printer, each with respective sounds, before I got bored of staff not paying any attention

- **Clear Desk and Clear Screen procedures need robust reinforcement:**
  Documentation, especially of a sensitive nature, left out and exposed on desks, as well as workstations left unlocked and unattended increase the potential level of attack. Files could be easily lifted from desks, and with reference to the example of Vishwanath, unlocked machines make it effortless to inject and run malicious contents from a USB drive

- **Poor preparation leads to poor performance:**
  Where policies and procedures are implemented within an organisation, most principally with Business Continuity and Clear Desk/Clear Screen, these must be routinely tested for

[17] No references available

* Disclaimer: Views expressed are the personal opinions of the author only and therefore cannot be attributed to Advent IM

effectiveness. If staff are ignorant of how to conduct themselves within a test scenario, this will be reflected in their reactions to a true event

- **As with anything, protection measures must be proportionate:**
  Criticality and sensitivity of whatever asset is to be protected must be reviewed, appreciated, and documented to gain a greater sense of the level of protection to be applied. Much like with my opening quote; if it is of value, then it must be afforded the appropriate level of security

- **Seek independent advice:**
  There is an ever-growing assortment of controls and solutions which can be adopted, but are not always suitable or compatible with business operations. Where expert, tailored recommendations are needed, they should be sought and implemented where possible

Concluding Remarks

As has been presented within this whitepaper, information security is steadily propagating news articles with stories being written and shared surrounding the latest data breach or sophisticated attack. Due to the logical means by which these attacks take place, emphasis and effort has been spent on a logical response. As such, there has been a rise in organisation's seeking third-parties to assess their IT infrastructure through penetration tests or ITHCs. Physical security, as a result, has fallen by the wayside with varying degrees of appetite and support for assurance activities.

Physical Red Teaming, as a potential solution, should be seen as a supplementary measure to penetration testing. With commentators discussing the idea of the convergence of cyber and physical security, evidenced through the IoT, control validation techniques must also embrace both of these elements. Subsequently, it is imperative that organisations seek an independent evaluation. An objective perspective of any mitigating factor that an organisation has in place will assist in defining improvement strategies, as well as provide a sense of confidence that valuable assets are being appropriately protected.

To conclude with a rhetoric that is often attributed to cyber-attacks, but is also relevant for physical security; *"it is not a matter of 'if' but 'when', and when it does happen, is your organisation prepared?"*

advent-im.co.uk

0121 559 6699

0207 100 1124

@Advent_IM

bestpractice@advent-im.co.uk