12-5-2006

Risks and responsibilities in establishing a wireless network for an educational institution

Leigh Knights
Edith Cowan University

Matt Fonceca
Edith Cowan University

Georgina Mack
Edith Cowan University

Andrew Woodward
Edith Cowan University

DOI: 10.4225/75/57b65d583476f
4th Australian Information Security Management Conference, Edith Cowan University, Perth, Western Australia, 5th December, 2006

Risks and responsibilities in establishing a wireless network for an educational institution

Leigh Knights
Matt Fonceca
Georgina Mack
Andrew Woodward

School of Computer and Information Science
Edith Cowan University
Perth, Western Australia

a.woodward@ecu.edu.au

Abstract

A wireless network solution is generally implemented when the bounds of walls of buildings and the constraints of wires need to be broken. Wireless technologies provide the potential for freedom of mobility which is undoubtedly a convenience for organisations in today's market. The security of a wireless network is crucial for data integrity, especially when the data is not secured by the insulation of wires. While data is being transferred across a wireless network, it is vulnerable. There is no room for error, neglect or ignorance from an organisation, as a breech of data integrity can be devastating for both businesses and institutions. Securing a wireless network needs to be treated as mandatory for educational institutions, and not just as best practice. With both legal and financial consequences for a breech of data integrity and the data protection act, education institutions need to realise the legal obligations and liabilities they face with respect to the sensitive data and information traversing their network.

Keywords

Wireless networks, education, data protection act, legal obligations, liability

INTRODUCTION

Educational institutions whether they be primary, secondary or tertiary, are likely to have a considerable amount of sensitive data and information that needs to be kept secure. Student records, contacts details, reports, administrative and accounting data are just some key elements of information that needs to be kept confidential. Can implementing a wireless network for such establishments lead to a breech of data confidentiality? If so, who is liable if this confidential information is leaked? Security is obviously needed for a wireless solution, but ignorance and lack of awareness and education can have serious consequences for such institutions. Is the cost of securing a wireless network worth a compromise in data integrity? Educational establishments need to be made aware of their legal obligations and liabilities in regards to potential leaks and breeches in relation to implementing a wireless network solution. The question that needs to be put to the clients is how valuable the information that they possess is, and what are they willing to do to protect it.

Security breaches in the USA are common place in the education system, and that security breaches across the USA are almost a weekly occurrence (Miller, 2006). In April of 2005, the Tufts University in Boston reported a breach to their fund raising and donor database after noticing abnormal activity on a server in October and December (Roberts, 2005). The Tufts University suspicions were raised after it was identified the breach that occurred earlier that year in March was identical to the ones in October and December. The Tufts University in Boston was not alone in reporting these sorts of security breaches, other universities include California State University, Chico, and the University of California, Berkeley (Roberts, 2005). Initially the Tufts University did not report the breach but was forced to after the second and third attacks were identified later that year. As a precaution the University sent out letters to the 106,000 alumni in the database warning them of the information leak but stated the University could not confirm that any of the information contained in the database was actually accessed or that information was not copied and then misused. The recipients of the letters were encouraged to take precautions by filing fraud alerts with their financial institutions and to check for any unusual activity in their name (Roberts, 2005).

In September 2006 the University of Minnesota reported that 2 new computers were stolen, it is believed the value of the computers rather then their data content is what was desired. Unfortunately the 13,084 data records contained on the 2 computers held personal information on students and their academic records. Of the 13,084 personal records, 603 records also contained Social Security Numbers. As a result of the computers being stolen, the University of Minnesota put staff through mandatory data-security training (United Press International, 2006).

In May 2006 the Sacred Heart University in Fairfield, reported one of its computers had been hacked, resulting in the potential compromise of personal data belonging to 135,000 alumni and prospective students (Vijayan, 2006). The IT staff discovered that a hacker had installed a Rootkit designed to bring down one component of a server, which was taken off line as soon as the discovery was made. The Sacred Heart University stated there is no indication that the information has been misused but informed the 135,000 alumni and prospective students affected by the breach.

This paper will explore the problems with establishing a wireless network for an Australian educational institution. The flaws and problems with wireless network security are examined, and responsibilities of the educational facility in relation to privacy are also discussed.

WIRELESS NETWORK SOLUTIONS

A wireless network solution is generally implemented when the constraints of wires need to be broken. Wireless technologies provide freedom of mobility which is undoubtedly a convenience for organisations in today's market. The ability to roam from building to building without disconnecting from the network is the type of mobile technology that businesses are beginning to now consider a standard feature in their network topology.

Studies have found that there are over 20 million wireless devices in service globally (Hale, 2006), showing the world wide adoption of wireless technologies. Wireless access points are wireless local area network (WLAN) transceivers that serve as a focal point of a stand-alone wireless network, or as the connection point between wireless and wired networks. These access points are able to seamlessly integrate with the existing wired network simply by connecting the hardware to the existing routing infrastructure. Access points help create network flexibility, and are now an affordable, efficient and transparent means of connecting people (Wireless News, 2006). Although the initial setup is fairly simple, the security and authentication setup is far more challenging.

With the correct equipment for the job, and the proper encryption and policies implemented, organisations will discover a balance of security, maintainability and a robustly performing wireless configuration. There is great emphasis on security in the present day, with good reason too; where there is vulnerability, there is a person ready to exploit and take advantage of it. Wireless networks are more vulnerable to breeches than wired networks, given their nature of transmitting data through the air from destination to destination (ref).

The obstacle that many organisations face implementing a wireless network is obtaining a balance between robust security and staying on a strict budget. Although, the costs between wired and wireless can vary, it is cheaper to install cable during the construction of a new building, but it is more expensive to install the wires if the building is already standing (Dennis, 2002). Depending on the situation, an implementation of a wireless network may be financially beneficial or cost effective to an organisation. The negative points to wireless networks involve the very real risk of a security breech and the loss of the organisations data integrity. Security risks like interception and theft of service, can omit a cloud of uncertainty on the implementation of wireless networks (Pfleeger and Pfleeger, 2003).

WIRELESS NETWORK SECURITY

The security of a network is crucial for data integrity, especially when the data is not secured by the insulation of wires. While data is transferring through a wireless network, it is vulnerable out in the open air. There is no room for error or neglect from the organisations as a breech of data integrity can be devastating on a business or institution. Education agencies that thrust into the world of computer networks and electronic communications are often unprepared for the related security risks and are unaware of many of the strategies that can protect their system (Pangborn, 2003). The importance of security on a wireless network and the use of different techniques of authentication, fortification and secure settings can prevent these threats and breeches.

Often network administrators overlook the importance of wireless security. In avoidance of this, administrators need to understand the strengths and weaknesses of wireless so they can take the appropriate steps to address those security issues (Neoh, 2003). The current security standard for protocol-based authentication for wireless networks is 802.1x. This was originated from the wired networking world and has been 'retrofitted' for wireless local area networks because of the deficiencies with the wired equivalency protocol (WEP), 802.1x is one of the top tools for credentialing users (Wailgum, 2006).

802.1 x authentication is based on the extensible authentication protocol (EAP). It uses encrypted tunnels to transfer information, such as user names and passwords, between the device and the network. Although an intruder can monitor the exchange of data over the air, the data inside the encrypted tunnel is very difficult to intercept. Because EAP is used on wired networks, it's attractive when project teams are pushing for a unified network strategy. Its mutual authentication ability gives users the added protection when they connect to the network, and ensures what they are seeing is actually legitimate, and not an intruder's fake access point. To help fight with such a threat, client-based software from vendors such as AirDefense and AirMagnet can help with authentication issues as well (Wailgum, 2006).

WIRELESS AT WEST AUSTRALIAN SCHOOLS

A recent case study on a West Australian school indicated one educational institution that is looking towards investing in a wireless network. While the benefits of a WLAN were clear, the security risks associated with implementing wireless into an educational environment were not. In fact during initial discussions with the college security was not mentioned at all, instead, ease of use, coverage and minimal costs where the main priorities. It was not until they were informed that by law they are obligated to protect confidential data and that they can be held responsible for any breeches that security became an issue. This oversight has become more common as many educational institutions looking to implement wireless networks are more concerned with increasing, not restricting user access to data.

The question then became how to provide a secure scalable wireless solution that was relatively inexpensive to setup and maintain while still remaining user friendly and require little administrative maintenance?

The School's solution was the implementation of a WLAN protected by Dynamic WPA and PEAP with MSCHAP v2. While it is known that PEAP is vulnerable to Man in the Middle Attacks and password harvesting, additional safeguards such as an Intrusion Detection System and SPI firewalls were put in place to help mitigate PEAP's vulnerabilities. Numerous wireless policies and best practices were also put in place to add to the overall security of the solution.

While this solution made the network relatively safe from electronic based attacks, it was discovered that due to the nature of high school environments and relatively small staff size, social engineering protocols were being ignored and staff and students were not only sharing their usernames and passwords, but also leaving their machines logged in and unattended for extended periods of time. This presented a major concern in that while all necessary steps were taken to secure the newly implemented wireless network, a potential attacker could circumvent security by simply using an unattended machine or pose as a new staff member and ask other staff members for their username and password. The solution to this problem came in the form of the LimitLogin Utility and the Windows 2003 Resource Kit, both available from the Microsoft website.

The LimitLogin utility was used to restrict users to a single login session which in turn effectively stopped the sharing of user names and passwords as in doing so, users were in effect hindering their own access to the network. The problem of leaving logged in machines unattended was solved via the use of the winexit screensaver bundled in the Windows 2003 Resource Kit. This screen saver enabled the machine to automatically log off after a preset number of minutes of inactivity.

The LimitLogin Utility and WinExit Screensaver combined with the security protocols in place with the wireless network, ensured protection against the electronic and social engineering avenues of attack.

DATA INTEGRITY

Lost or compromised data is increasingly unacceptable in online systems. Following a failure of a system involving business-critical data, virtually any executive today would expect and demand that the application promptly resume operations with a database that is complete, accurate, consistent and restartable (Winter, 2000). Business and institution reliance on the networks they use, and the data and information that resides on them, is extremely high, ensuring the data within these networks is available, correct and not compromised is essential to business function and process. Data and data integrity protection is an integral part of network implementation and security. Managed security services give businesses and institutions an advantage where they cannot afford or do not want in house dedicated IS staff. However, attacks are volatile and debilitating to such businesses and institutions, and providing a multi-layered security approach can protect business critical environments (M2 Presswire, 2006).

When discussing the importance of data and data integrity within educational institutions, there are many different types of information that need to be considered for protection. Some examples of such information types are emails, human resource information such as financial details and payroll, personal details, address books, student information such as profiles, grades and enrolment details. This list is by no means exhaustive, but these information types show the key aspects of data found in educational institutions that are heavily targeted by intruders.

Schools obtain information on pupils and members of staff and in doing so must follow the requirements of the 1998 Data Protection Act. This means that data held about pupils must only be used for specific purposes that are allowed by the Act. These rules regarding personal data also apply to employees, whether they are teaching or non-teaching staff (Wagland, 2004). A breech by an intruder, causing the data to be stolen, changed or deleted is in fact a breech of the Act. The question then resides on who is liable or accountable for the breech, the intruder, or the persons responsible for the security of the network? The education institution needs to be aware of the data protection act so the real threats can be taken into consideration. Ignorance, or, simply just neglecting the protection act, and its threats, cannot become an excuse when the ramifications of doing so can be deemed a very serious and grave offence. Measures need to be put in place in order for security breeches and the loss of data integrity to be monitored, controlled and stopped.

THREATS

Threats related to WLANs are considerable, many in number of different threats, and they continue to grow. Many attacks and threats must be taken into consideration when implementing a wireless network. It is crucial in any educational institution to implement countermeasures to obvious threats to ensure data integrity and confidentiality. In educational institutions, a compromised wireless network can prove not only costly but detrimental to its overall operation. Understanding these threats is an important task in implementing policies related to ensuring a secure wireless environment.

Passive wireless attacks

A Passive Attack does not intrude upon the wireless network nor is it readily detectable with the tools available today. Wireless networks, being broadcast medium, are naturally vulnerable to attack. If access points used on the network are only configured with the factory defaults attackers using sniffer software will be able to see and obtain data from the traffic being passed over the network (Woodward, 2005). NetStumbler, as well as other readily available tools are downloadable from the internet and are used to detect and gain access to access points using the SSID's which are broadcast and detected within an unsecured WLAN.

Social Engineering

This is another common treat in any WLAN environment which is sometimes overlooked. Even though it may seem like a low risk threat, it is ultimately an effective way to gather information to gain unauthorized access. It has been found that charm, and good social skills, intertwined with persuasiveness can result in achieving successful intelligence gathering and access for unauthorised personnel. Social engineering is the human weak link of computer security and awareness of these threats need to be addressed to the users. Honest people will be willing to be apart of the solution and not the problem. (Musthaler, 2006).

Rogue Access Points

Rogue Access points refer to actions of perpetrators, whether it is employees, or unauthorised individuals who intentionally install access points to gain relatively easy access in a wireless network. Rogue access point incorporate threats such as eavesdropping to steal sensitive information either remotely or locally. Serious breeches can occur and result in disastrous ramifications if rogue access points are configured with a passive SSID and MAC access list as they may be difficult to detect (Woodward, 2005).

Man-In-The-Middle Attacks

Within a WLAN environment, a person can easily monitor 802.11 frames sent over the WLAN and easily fool the network, by breaking the signal and presenting themselves as a legitimate access point. These attacks on a network work when a Man-In-The-Middle attacker appears as the access point and becomes a proxy between the client and the real access point. This is becoming a more common and predictable type of attack and strong client and server authentication need to be in place to survive the internet (Business Credit, 2006)

These are some of the major threats to the wireless networks, and data integrity, of educational institutions. There are many other types of threats that can involve such things as lack of true authentication, SSID broadcasting, session hijacking, poor physical location of access point in a building and Denial of Service attacks. All these types of attacks and flaws are serious threats to a wireless network in an educational institution, where breeches can incur serious ramifications and legal liabilities.

LEGAL OBLIGATIONS AND LIABILITY

Securing a wireless network isn't just best practice for data integrity for educational institutions, but a mandatory process in order to comply with the laws put in-place. With harsh consequences carried out for a breech of data integrity and the data protection act, education institutions need to realise the legal obligations and liabilities they face with the sensitive data and information on their network. Neglection and ignorance are inexcusable reasons for the failure of data protection, as under the act, schools are 'data controllers'. The data controller must ensure the data is fairly and lawfully processed, processed for limited purposes, that the data is adequate, relevant, accurate, and not excessive, kept no longer than necessary, processed in accordance with the data subjects rights and that the data is well secure (Wagland, 2004).

All types of information must be covered and included with the consideration of the data protection act and its best practises. Personal information is such information that is about an identifiable individual that can include, but not limited to, fields like age, gender, race even medical and educational history (Buy Inc. Attorney, 2006). Such information can be used against the individual targeted if the network is breeched and the data is compromised. Education institutions are liable for this information and they are obliged to protect the data transferred throughout the network.

As discussed previously, there are numerous threats to data protection and integrity from outside wireless networks. Education agencies must be prepared for every threatening scenario ranging from a careless employee walking away from a computer station that is logged onto a sensitive data site to a hacker trying to break into the institutions system to physical destruction of the network by a natural disaster (Pangborn, 2003). An education institution involved in maintaining a computer network, especially one with Internet access, should have policies to identify and resolve system vulnerabilities and in so doing reduce the risk of liability.

Educational institutions are legally obligated to protect data upon their network and databases as they are liable for any breech that occurs upon that system. Educational institutions need to implement appropriate technical and organisational measures to safeguard the data against risk of loss, damage, destruction of or unauthorised access to personal information (Buy Inc. Attorney, 2006). Such institutions need to address these risks and provide satisfactory I.T security controls and measures. In addition to wireless security measures, policies such as data protection and data privacy policies, interception and surveillance policies as well as auditing policies may need to be put in place as an additional safeguard.

All information stored within the network needs to be accurate and uncorrupted. The emphasis on this form of data integrity breech revolves around student's grades and subject material and marking (Buy Inc. Attorney, 2006). Educational institutions are obligated to provide sufficient encrypting and authentication for users residing on the network. Security verification and authentication measures ensure correct identity management and validation. Besides identity management, a records management policy can apply an effective governance of these sensitive types of data, where version control is a government standard for auditing purposes which educational institutions are obligated to have implemented.

Australian data protection statutes and standards come from the Privacy Act, 1988 and the Privacy Amendment (Private Sector) Act 2000 (Federal Privacy Commissioner 2006). The Data Protection Act attempts to cover the collection, storing, editing retrieving, disclosure, archiving and destruction of data. By using the Data Protection Act within an educational institution as a framework, ramifications from data integrity breeches can be avoided. A secure wireless network ensures the educational institutions obligations for protecting the data within the system. The company with the network system are liable for establishing voluntary and mandatory mechanisms or procedures which will uphold the right to privacy (Buy Inc. Attorney, 2006). This must be effectively governed by all bodies involved, which includes, educating all users so that they understand their rights in terms of the data protection act. Appropriate technical and organisational measures need to be in place to ensure the safety of the data against the risk of damage, modification, loss, deletion, destruction or unauthorised access to the data within the system.

If the legal obligations of the data protection act are not complied with, this institutes a criminal act. Privacy is extremely important in many countries as a breech of any kind on the privacy act is a grave criminal act. Failure to comply with an act of privacy is considered a criminal offence, as such, enforcers of the act can assist individuals and groups affected by a breech of privacy and data integrity by assisting with the claiming of compensation from the responsible party for any damage inflicted (Buy Inc. Attorney, 2006). The data protection act, although strict in nature, also takes a more flexible approach if industries and institutions develop their own 'codes of conduct' which can be overseen by a supporting regulatory agency. Overall, the legal liabilities and obligations of education institutions, wanting to implement a wireless network, are considerable, which can cause serious ramifications and penalties if a breech of data integrity and, furthermore, privacy is experienced.

RECOMMENDATIONS

There is no doubt that with hardware and software technologies becoming easier to implement, many inexperienced individuals are implementing technologies, such as wireless networks, without considering the security needed behind it. For an educational institution recommendations and best practices should be addressed and implemented to help monitor, control and prevent breeches of the system.

There are undoubtedly many areas of security that need to be covered when implementing a wireless network. Firstly, a security assessment needs to take place, where flaws need to be identified and rectified within the current system. This includes the testing of hardware, software, and currently implemented policies. Wireless networking security measures include steps such as shutting off Service Set Identifier (SSID) broadcasting and using an SSID that does not identify the institution by name (Pangborn, 2003). Another recommendation that can help insure that breeches do not occur is changing the default SSID name from the default factory settings as well as the default passwords (AGAGD, 2006). Updating the firmware on access points and other hardware used and using WPA2 encryption is also best practise.

Enabling MAC address filtering also helps with data integrity as this allows access to devices containing only certain MAC addresses. MAC address filtering isn't fool proof, but it can slow down intruders and acts like a hurdle in a potential attacker's way (AGAGD, 2006). A recommendation to educational institutions implementing a wireless network is to place the wired portions of the individual access points on separate VLANs (Virtual Local Area Networks) which will allow the system administrators to separate traffic and lessen the access a potential hacker has on the network (AGAGD, 2006;Pangborn, 2003). Firewalls and port blockers are also other strong security implementations for wireless networks.

It is also recommended that for enterprise level networks such as educational or business, some form of 802.1x authentication is highly recommended as it provides a high degree of security when combined with Windows 2003 Server's Active Directory and Remote Authentication Dial In User Service (RADIUS).

Implementing policies on the network is just as important as the recommendations stated above. Implementing a set of policies on wireless network security and clearly identify the ownership of those policies (Neoh, 2003). Reviewing those policies regularly, to ensure security control when new risks are identified, is essential. Such policies should include records management policies, data protection and data privacy policies, interception and surveillance policies, and auditing policies. These set of policies limit unnecessary data transfer and help lock down the network in order to maintain a satisfactory standard of data integrity ensuring the framework of the data protection act is upheld.

The recommendations stated above are not exhaustive, but it gives an idea of the security implementations available in today's security and network technology market. With a balance of proper hardware and software security tool implementation and strict security policies, the strength of the security implementations for a wireless network can ensure a robust defence against the threats facing data integrity. Ensuring the confidentiality, availability and integrity of data on a wireless network of an education institution is paramount for the sensitive data that lies within the system.

CONCLUSION

Educational Institutions are just one of many business organisations that are regularly targeted by intruders. They hold vast amounts of sensitive data on their systems including grades, financial data, marking information and human resource data are other types of information targeted by intruders. Ensuring data integrity and privacy is essential in order to comply with the data protection act and as the case studies have shown, there are serious and real ramifications to breeches of the act. Recent legislation on data protection and freedom of information has given greater rights to the individual and alongside them; greater responsibilities on those hold personal data, whether on paper or electronically (Wagland, 2004).

Educational institutions need to be aware of the legal obligations and liabilities faced when implementing a wireless network as breeches can be considered criminal acts and serious consequences are in place for if the data protection act is neglected and ignored. It has been then suggested that wireless security implementations need to be put in place to tackle these threats to data integrity. Security needs to be analysed and a proactive approach needs to be used in order for successful data privacy and protection within wireless networks in an educational institution.

REFERENCES

Australian Government Attorney-General Department. (2006). Wireless Security – Information for CIO's., URL http://www.ag.gov.au/agd/WWW/rwpattach.nsf/VAP/(7A188806B7893EBA0402BC1472412E58)~Wirel ess+Security+-+Overview+CIOs.doc/$file/Wireless+Security+-+Overview+CIOs.doc accessed 1 October 2006

Business Credit. (2006). Man-In-The-Middle Phishing Attack Sucessful Against Citibank's Two-Factor Token Authentication. Business Credit 108 (9). 2.

Buys Inc. Attorneys. (2006). Privacy and Data Protection Guide 2006, URL http://www.buys.co.za/ accessed 1 October 2006

Dennis, A. (2002). Networking in the Internet Age. New York: John Wiley & Sons, Inc.

Federal Privacy Commissioner (2006). Federal Privacy act, URL http://www.privacy.gov.au/publications/privacy88_061006.pdf accessed 1 October 2006

Hale, G. (2006). At long last, wireless is ready. Intech. 53(7), 7.

M2 Presswire. (2006). Arbor Networks: Arbor Network teams with Service Providers to answer growing enterprise demand for managed security services. M2 Presswire. Coventry: January 9th, 2006.

Miller, N. (2006). Data leaks under review. Sydney Morning Herald. Sydney.

Musthaler, A. (2006). How Social Engineering Sinks Security. Network World. 23(39). 45

Neoh, D. (2003). Corporate Wireless LAN: Know the Risks and Best Practices to Migrate them, URL http://www.sans.ord/reading_room/whitepapers/wireless/1350.php accessed 1 October 2006

Pangborn, J. (2003). Weaving a Secure Web around Education, URL http://nces.ed.gov/pubs2003/secureweb/ch_6.asp accessed 1 October 2006

Pfleeger, C.P & S.L. (2003). Security in Computing. Pearson Education Inc. Upper Saddle River, New Jersey

Roberts, P. (2005). "Tufts warns 106,000 alumni, donors of security breach.", URL http://www.computerworld.com/securitytopics/security/story/0,10801,101043,00.html accessed 1 October 2006

United Press International. (2006, 09 Sep). "U. Of Minnesota Reports Computer Theft, URL http://news.usti.net/home/news/cn/?/news.crime.theft/1/wed/bu/Uus-computertheft.R8BP_GS9.html accessed 1 October 2006

Vijayan, J. (2006). "Two more organizations report data breaches", URL http://computerworld.com/action/article.do?command=viewArticleBasic&articleId=9000878&intsrc=article_more_side accessed 1 October 2006

Wagland, S. (2004). Data protection and security: a summary for schools, URL http://schools.becta.org.uk/ accessed 1 October 2006

Wailgum, T. (2006). The Security Plan for Your Wireless LAN; Take advantage of the latest security tools and keep your users informed if you wan to achieve wire-free bliss. CIO 19(17), 1.

Winter, R. (2000). It's About Data Integration. Intelligent Enterprise. 3(1), 84-86.

Wireless News, (2006), Cisco Wireless Goes Green with Hearst Tower in NYC. Wireless News. Coventry: September 21st, 2006

Woodward, A. (2005). Recommendations for wireless network security policy: an analysis and classification of current and emerging threats and solutions for different organisations. Proceedings of 3rd Australian Information Security Management Conference, Edith Cowan University, Perth Western Australia.

COPYRIGHT