University of Essex | Online

# Seminar 1: Blog Post

**Course:** MSc Computer Science

**Module:** Secure Software Development (Computer Science)

**Assignment:** ePortfolio

**Date:** Saturday 30th October 2021

**Student ID:** 126853

## Post:

Cybersecurity is the art of safeguarding computer networks, and the data consisted within them from external threats seeking to cause damage or disruption (Lewis, 2006). Bulai et al. (2019) stated that 95% of security incidents were directly attributed to human error. Unsurprisingly, a lot of these incidents are likely to happen due to actions from staff within the business.

One step to avoiding cybersecurity incidents within the business is by implementing robust access control policies. Such policies would ensure that only the minimum level of access for an employee to perform their job reliably is provided (Coronado & Wong, 2014). This action would result in a lower residual risk due to the lower chance of a user-account breach providing a significant level of system access.

Many technical attack prevention methods are available to a business, such as the implementation of Antivirus tools, Firewalls, Whitelisting and Monitoring (NCSC, 2015). These should be combined with a series of internal policies and training to ensure that staff are aware of the businesses expectations surrounding security. In most cases, a policy would include information surrounding minimum password requirements, usage of external storage devices, and the level of personal information/accounts that can be accessed on work devices (Personal emails/storage accounts).

When a series of preventative actions are taken, both on a technical and staffing level, you can reduce the likelihood of a cyberattack occurring against your business.

In some cases, this can ensure continued conformity with Government/Regulatory Body requirements – preventing a potential upstream loss of service (For example, PCI-DSS compliance).

## References:

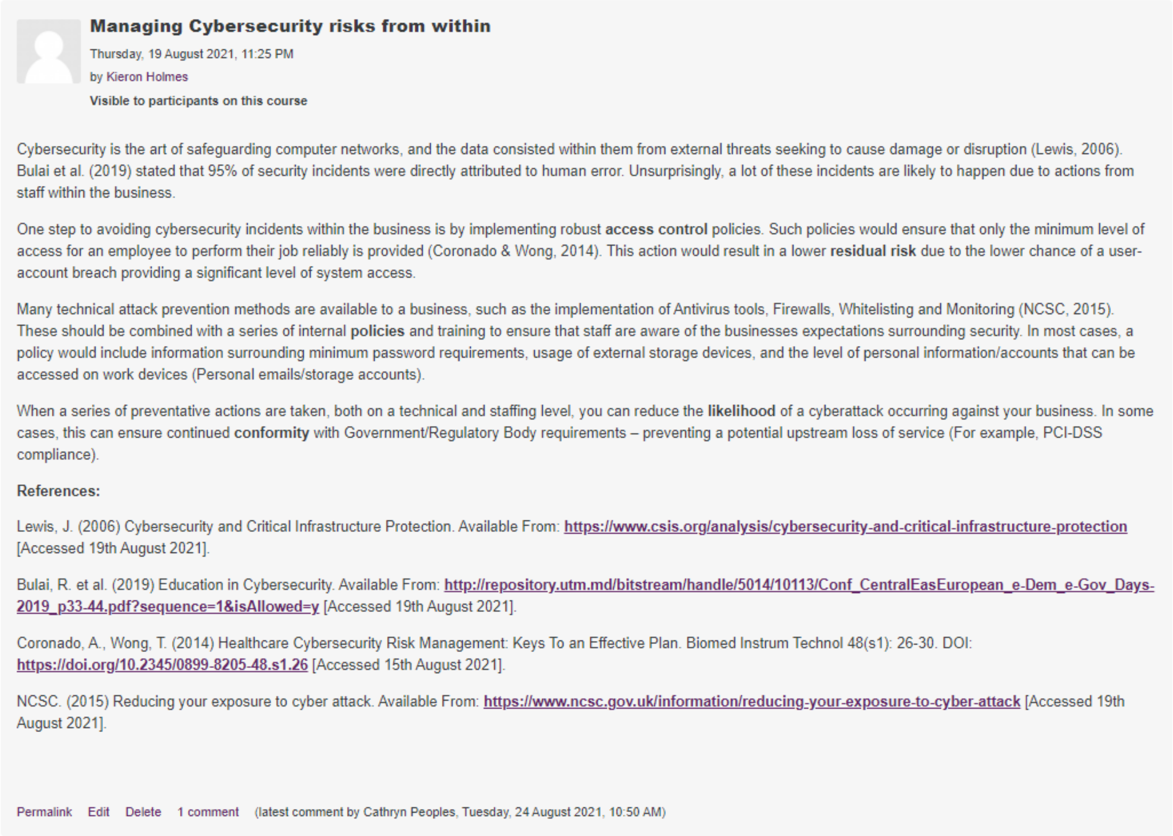
Bulai, R. et al. (2019) Education in Cybersecurity. Available From: http://repository.utm.md/bitstream/handle/5014/10113/Conf_CentralEasEuropean_e-Dem_e-Gov_Days-2019_p33-44.pdf?sequence=1&isAllowed=y [Accessed 19th August 2021].

Coronado, A., Wong, T. (2014) Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomed Instrum Technol 48(s1): 26-30. DOI: https://doi.org/10.2345/0899-8205-48.s1.26 [Accessed 15th August 2021].

Lewis, J. (2006) Cybersecurity and Critical Infrastructure Protection. Available From: https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection [Accessed 19th August 2021].

NCSC. (2015) Reducing your exposure to cyber attack. Available From: https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack [Accessed 19th August 2021].

# Screenshot:



**Managing Cybersecurity risks from within**

Thursday, 19 August 2021, 11:25 PM

by Kieron Holmes

**Visible to participants on this course**

Cybersecurity is the art of safeguarding computer networks, and the data consisted within them from external threats seeking to cause damage or disruption (Lewis, 2006). Bulai et al. (2019) stated that 95% of security incidents were directly attributed to human error. Unsurprisingly, a lot of these incidents are likely to happen due to actions from staff within the business.

One step to avoiding cybersecurity incidents within the business is by implementing robust **access control** policies. Such policies would ensure that only the minimum level of access for an employee to perform their job reliably is provided (Coronado & Wong, 2014). This action would result in a lower **residual risk** due to the lower chance of a user-account breach providing a significant level of system access.

Many technical attack prevention methods are available to a business, such as the implementation of Antivirus tools, Firewalls, Whitelisting and Monitoring (NCSC, 2015). These should be combined with a series of internal **policies** and training to ensure that staff are aware of the businesses expectations surrounding security. In most cases, a policy would include information surrounding minimum password requirements, usage of external storage devices, and the level of personal information/accounts that can be accessed on work devices (Personal emails/storage accounts).

When a series of preventative actions are taken, both on a technical and staffing level, you can reduce the **likelihood** of a cyberattack occurring against your business. In some cases, this can ensure continued **conformity** with Government/Regulatory Body requirements – preventing a potential upstream loss of service (For example, PCI-DSS compliance).

**References:**

Lewis, J. (2006) Cybersecurity and Critical Infrastructure Protection. Available From: https://www.csis.org/analysis/cybersecurity-and-critical-infrastructure-protection [Accessed 19th August 2021].

Bulai, R. et al. (2019) Education in Cybersecurity. Available From: http://repository.utm.md/bitstream/handle/5014/10113/Conf_CentralEasEuropean_e-Dem_e-Gov_Days-2019_p33-44.pdf?sequence=1&isAllowed=y [Accessed 19th August 2021].

Coronado, A., Wong, T. (2014) Healthcare Cybersecurity Risk Management: Keys To an Effective Plan. Biomed Instrum Technol 48(s1): 26-30. DOI: https://doi.org/10.2345/0899-8205-48.s1.26 [Accessed 15th August 2021].

NCSC. (2015) Reducing your exposure to cyber attack. Available From: https://www.ncsc.gov.uk/information/reducing-your-exposure-to-cyber-attack [Accessed 19th August 2021].

(latest comment by Cathryn Peoples, Tuesday, 24 August 2021, 10:50 AM)