What Influences People's View of Cyber Security Culture in Higher Education Institutions? An Empirical Study

5-6th October 2021

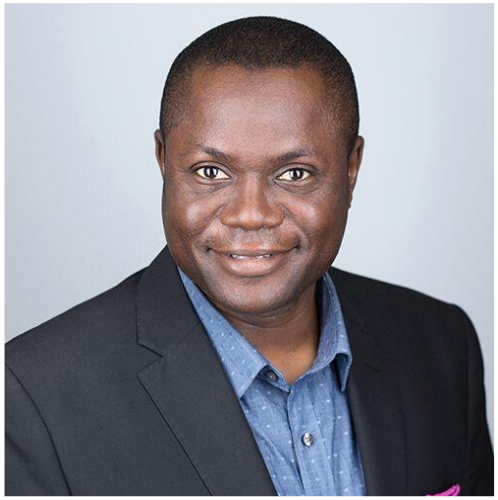
Tai Durojaiye | Dr Konstantinos Mersinas | Prof Dawn Watling

CYBER 2021 Barcelona, Spain

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Presenter Bio

Tai Durojaiye is a PhD candidate of information security at Royal Holloway University of London (RHUL). Tai's research interests are cyber security culture, security perception and behavioural aspect of cyber security.

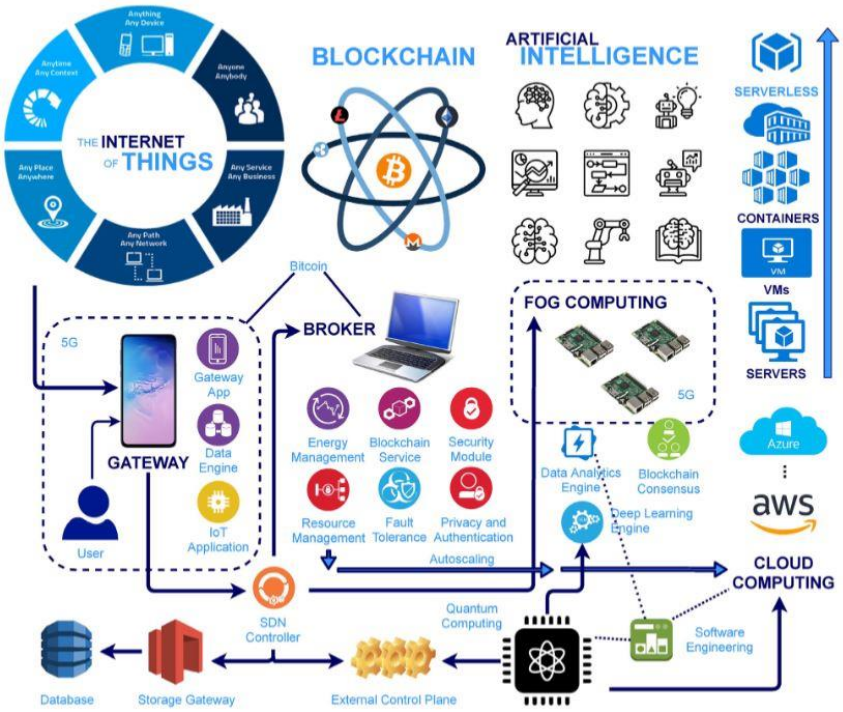


Before RHUL, Tai has extensive years of experience from the oil and gas industry working in risk and reliability and system engineering. He has a BEng in Electrical and Electronics Engineering (Brunel University) and MSc in Telecommunications (University College London).

Tai is a chartered engineer (CEng) and an ISO 27001 ISMS Lead Auditor.

LinkedIn https://www.linkedin.com/in/taidurojaiye

Introduction



(Gill et al, 2019)

Industry Response to Security Breaches

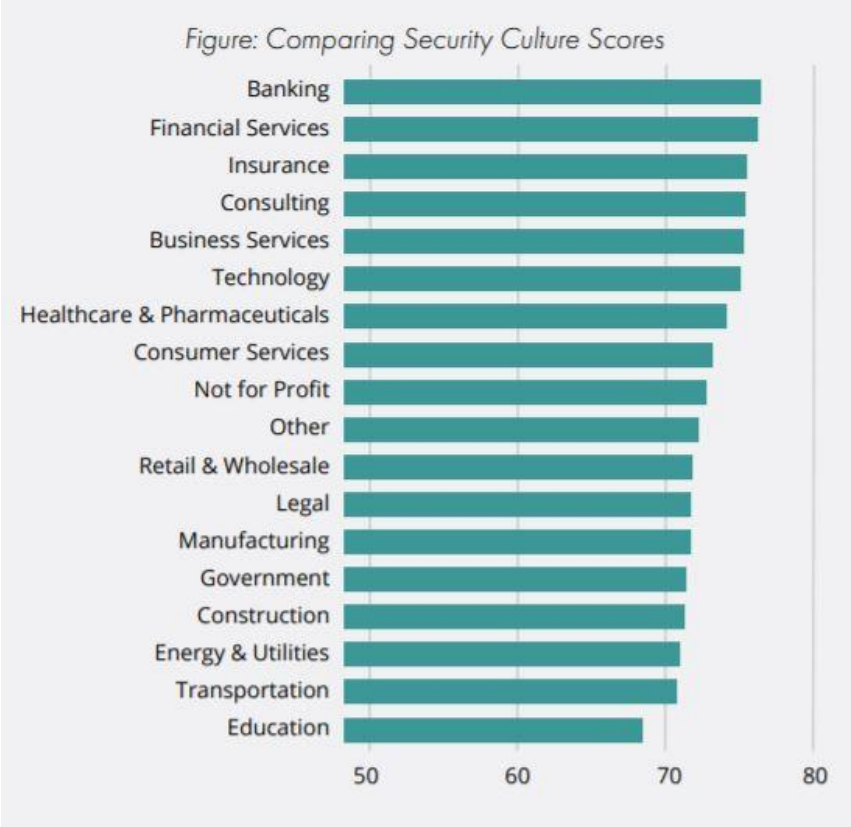
- Increased investments in technical controls (Safa, 2015)
- Increased investment in training and awareness
- No corresponding investments in cyber security in Higher Education Institutions (HEIs)
- Cyber security breaches continue to occur in HEIs
- Human aspects of cyber security is overlooked

New technologies | Increased attack surface | Information security challenge

Education Sector: Higher Education Institutions (HEIs) & the Challenges

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Comparing Security Culture Scores



- Education sector has the poorest security culture score amongst many sectors (Roer et al, 2020)
- Cyber attacks constitute a threat to UK HEIs (Chapman, 2019)
- UK HEIs are not well prepared to defend against and recover from cyber attacks (IBM CS Int Index, 2015)
- Users pose threats to the security of HEIs' assets
- Lack of understanding on how to foster cyber security culture (CSC)

(Roer et al, 2020)

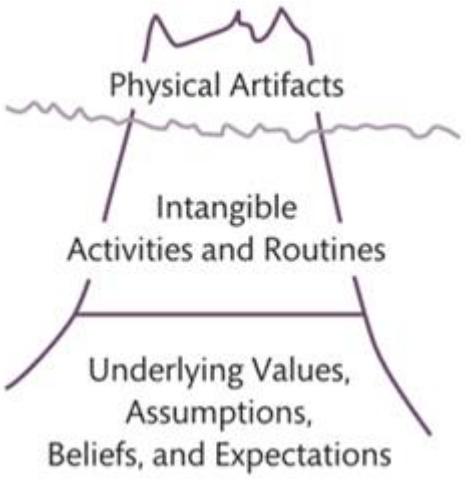
Why are UK HEIs being targeted by Cyber Attacks?

- UK HEIs hold a wealth of information e.g. high-value research data
- HEIs have financial/personal information of their staff, students, alumni and donors
- UK HEIs are considered as easy targets for cyber attacks
- Cyber security breaches have been reported at UK universities (Greenwich and Edinburgh) (ICO, 2018; Sanderson, 2018)
- Empirical studies are needed on CSC in UK HEIs

Organisation and Security Culture

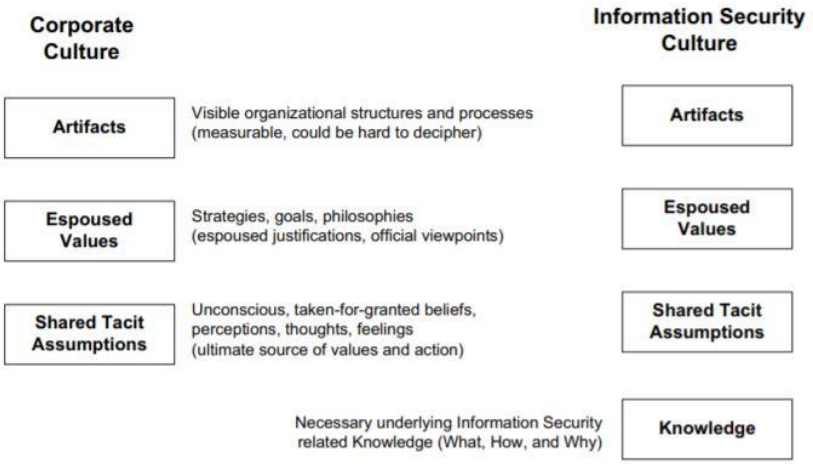
ROYAL HOLLOWAY UNIVERSITY OF LONDON

Schein's cultural iceberg



(King and Lawley, 2013)

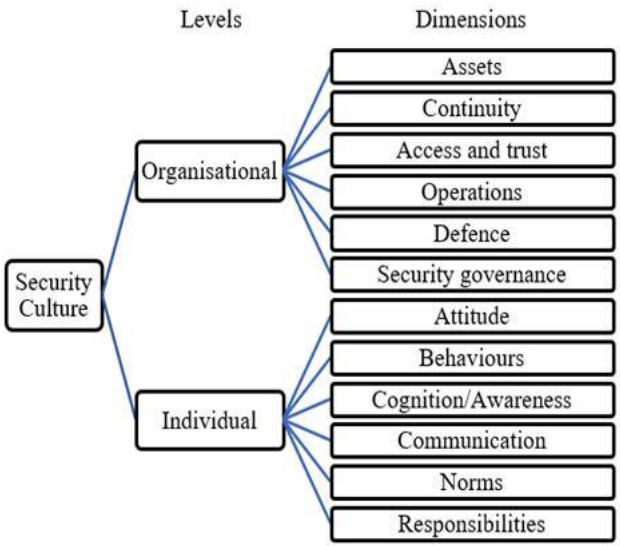
Schein's expanded model



(Niekerk & von Solms, 2010)

Cyber Security Culture Model & Dimensions

A Comprehensive Security Culture Model



(Georgiadou et al, 2020)

Dimensions of Cyber Security Culture

Dimension	Definition
Attitude	The feelings and beliefs that employees have toward the security protocol
Behaviours	The actions and activities of employees that have direct and indirect impact on the security of the organisation
Cognition/ Awareness	Employees' understanding, knowledge, and awareness of security issues and activities
Communication	The quality of communication channels to discuss security-related topics, promote a sense of belonging and provide support for security issues and incident reporting
Compliance	The knowledge of written security policies and the extent that employees follow them
Norms	The knowledge of and adherence to unwritten rules of conduct in the organisation
Responsibilities	How employees perceive their role as a critical factor in sustaining or endangering the security of the organisation

(Roer et al, 2020)

Empirical Study of Cyber Security Culture in UK HEIs

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- To highlight the current problems in UK HEIs through a practical approach
- The approach is to allow pertinent issues of security culture to emerge
- Focused on three UK HEIs in the south of England with similar characteristics
- Student numbers in the HEIs are between 10,000 and 20,000

Empirical Study - Methodology

ROYAL HOLLOWAY UNIVERSITY OF LONDON

- Target group comprises three senior management members, six academics, seven professional services/administrative staff and three PhD students
- Nineteen interviews were conducted (approx. 30 minutes each)
- Questions based on security perceptions, governance, devolution, university structure and culture, training and development, security of information and records
- Transcribed interviews were assessed by content analysis, with support of NVivo software

Results

Communication

Finding 1: Lack of systematic communication from the IT team to users

Question: How likely are you or your colleagues to comply with the university's IT and cyber security expectations?

"That sounds a little bit weak because the expectations are probably not very well defined"

"there is a lack of systematic communication between the IT services regarding cyber security to staff in general"

"I don't even know that. So, I would just like them to be a bit more clear"; "So I feel there's a real [problem], everything is very opaque"

Finding 2: Collaboration problems exist between the IT team and academics

Question: How protected do you think the university is from cyber security attacks?

"I try to work with them and to offer help and to try to increase the level of communication and collaboration, that has proved to be difficult"

Results

Communication (continued)

Finding 3: Communication is impersonal

Question: To what extent do you think there is fairness to users in how the IT department apply cyber and information security?

"I don't like the fact that [..] you don't ever get a signature, you have a conversation with someone over a few emails and you don't know who you're talking to"

Policies and Frameworks for Guiding Cyber Security Behaviour

Finding 1: Lack of enough policies/frameworks

Question: Are you aware of any workarounds that people have developed to bypass security policies and processes?

"I don't think there are enough, policies and processes in place that people would want to work around it"

"there is nothing to stop me sending a personal email from my work account, so we don't have anything, I believe, in our terms or policies that prevent you from doing that".

Results

Policies and Frameworks for Guiding Cyber Security Behaviour (continued)

Finding 2: *Lack of prioritisation*

Question: Is there a two to three years strategy plan for information security?

"I think one of the challenges [the university] has had around cyber security is that it has tried to do everything in terms of policy standard and technology all at once without any real sense of priority and without any real sense of priority based on an intelligent assessment of what the actual threat and risk is".

Moving Away from Phishing Exercises

Finding 1: Phishing exercises create more problems between the IT Team and users - distrust and resentment

Question: How beneficial do you or your colleagues think such exercise [phishing] will be?

"these kind of so-called realistic phishing exercise [..] will probably cause more problems than solving problems because it will cause some confusion, that can potentially even make the functionality fail".

"I'd find it a little bit, I guess in a way I'd feel it's a little bit violating that your own university is trying to phish you, even if it's to teach you a lesson, you know, it feels a bit off-putting".

Results

Moving Away from Phishing Exercises (continued)

Finding 2: Phishing exercises results used to blame others

Question: How do you think the phishing exercise was perceived by staff?

"for those that got caught, it would have been a bit of a wakeup call, I suspect, and it wasn't, ..if they think about it.. they should be quite glad that they clicked on something that was quite innocent and it was helping them raise awareness".

Training, Reinforced Training and Awareness

Finding 1: Cyber security training is lacking

Question: What training or security awareness courses do you have in place for users?

"No. There's no such thing as far as I understand. There's no cyber security training for staff or students as far as I'm aware".

"But I've not been on anything [portal] that says, "this is cyber security, and you shall do it"; "there isn't any, what I would describe as dedicated on-boarding training around students for cyber security and institution"

Recommendations

- Senior management to invest more in training and development for IT teams with specific focus on informing, engaging and persuading
- Senior management to prioritise the creation of a cyber security strategy, around which security policies could be built
- HEI leaders should engage academics' expertise within their institutions
- HEI leaders to investigate the problems caused by implementing phishing exercises, from users' perspective
- HEI leaders to prioritise and invest in trainings on social engineering/other human aspects of security

Conclusion

- Communication strategy, engagement and collaborative effort will help to develop a CSC
- Fostering CSC will reduce security breaches caused by human error
- Study limitation: More personnel could have been interviewed (Covid-19 barrier)
- Training could be geared towards individual user instead of applying a one-size-fits-all approach
- Future research could investigate how CSC could be measured in different HEIs

Bibliography

N. S. Safa, M. Sookhak, R. Von Solms, S. Furnell, N.A. Ghani, and T. Herawan. "Information security conscious care behaviour formation in organizations", *Computers & Security*, 53, pp. 65–78, 2015. Doi: 10.1016/j.cose.2015.05.012G.

N. Gcaza, R. Solms, "Cybersecurity Culture: An Ill-Defined Problem", IFIP World Conference on Information Security Education (WISE 2017) pp. 98-109, 2017. Doi: 10.1007/978-3-319-58553-6_9.

K. Roer, et al. "Measure to Improve, Security Culture Report 2020". [online] Available at: <https://www.knowbe4.com/hubfs/Security-Culture-Report.pdf> [Accessed 2 September 2021].

IBM, "IBM 2015 Cyber-Security-Intelligence-Index". Available at: https://essextec.com/wp-content/uploads/2015/09/IBM-2015-Cyber-Security-Intelligence-Index_FULL-REPORT.pdf (Accessed: 3 September 2021).

Ico.org.uk. *The University of Greenwich fined £120,000 by Information Commissioner for "serious" security breach*. [online] Available at: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/the-university-of-greenwich-fined-120-000-by-information-commissioner-for-serious-security-breach/> [Accessed 3 September 2021].

J. F. Van Niekerk, R. Von Solms, "Information Security Culture: A Management Perspective". Computers & Security, Vol. 29 (4), pp. 476-486, 2010.

D King, and S Lawley, Organisational Behaviour. Oxford University Press: Oxford, 2013.

THANK YOU

ROYAL HOLLOWAY UNIVERSITY OF LONDON