Business Ethics Are Office Ethics

Developing a cyber aware culture in an organisation & making a human firewall your strongest defence.

Executive summary

This report looks at the relationship between business culture and cyber security; specifically in relation to the ethical school of thought of the organization. A few schools of thought have been presented, as well as their pros and cons in relation to cybersecurity. A paradigm shift has been suggested that seems to support the literature and the needs of organizations. Ethical frameworks have a huge influence on cyber security, most notably in relation to human factors.

Table of contents

Acronyms and disclaimers

ACM	**Association of Computing Machinery**
GDPR	**General Data Protection Regulation**

Introduction

Statement of contribution

A key component of cyber security is the human factor, though it is often neglected (Rahman et al. 2021; Reid & Van Niekerk 2014). The hiring/training process, business procedures, and policies are all heavily influenced by the dominant schools of thought held by the business and are indicative of a business' culture (Sims & Brinkmann 2003). Businesses make many seemingly innocuous decisions that set the tone for future decisions and behaviours that

reverberate throughout the business (Banks 2016; Warner 2012; Wells & Spinks 1996). An organisations position and actions regarding privacy, management of utility vs security trade-offs, and commitment to transparency all stem from an organisation's ethical foundation (Banks 2016; Formosa, Wilson & Richards 2021). This foundation theoretically governs all human behaviours within the organization (Banks 2016; Wells & Spinks 1996).

In this report, we analyse how different business cultures may influences cybersecurity behaviours and outcomes focusing particularly on the human security components.

Literature review

There has been an ongoing and fractured discussion around the ethics of data (Formosa, Wilson & Richards 2021; Jurkiewicz 2018; Mittelstadt et al. 2016; White & Ariyachandra 2016). These discussions have largely been recorded in conference proceedings, or through attempts to bridge or extend existing codes (such as Australian Code for the Responsible Conduct of Research), or more numerously within organizations independently. While these discussions have gained collective uniformity over the years, they are still in their infancy in many industries (Formosa, Wilson & Richards 2021; White & Ariyachandra 2016). There are great economic drivers to collect and use data, but only over the last few decades has the threat of a cyber-attack been realized as a question of 'when,' and not 'if' (Škanata 2020). As the technology became more readily available and the benefits of data usage became fully realized, companies and consumers adapted, evolving into what we have today (Sharif & Ghodoosi 2022). As the world adapts, it is becoming more necessary for regulation and regular auditing (Hoofnagle, Van Der Sloot & Borgesius 2019). This need provided the ignition required to generate more uniform and meaningful debate. The GDPR was the outcome of such debate and is seen as the gold standard currently, though many argue it does not go far enough (Hoofnagle, Van Der Sloot & Borgesius 2019; Mantelero 2021). Currently consumer data is used as a product and sold with no economic benefit to the consumer. There are models available that remedy this inequality, but there is little incentive for their uptake (Line et al. 2020).

These discussions aim to be beneficial, but to whom may be inconsistent depending on the dominant school of thought and culture within an organization. There are a few dominant schools of thought in business ethics (*table 1*).

Table 1: An introduction to four major schools of thought.

School of thought	Description
Consequentialism (Utilitarianism and Stakeholder theory)	Largely focussed on the consequences of actions. Utilitarianism stipulates that the option that results in the greatest benefit among all stakeholders. Stakeholder theory is similar, but it operates on an organizational, and not an individual, level.
Deontology	Stipulates that there are intrinsic principles or rules that must be adhered to regardless of the consequences.
Virtue ethics	Stipulates that individuals should strive to cultivate virtuous qualities. And that in doing so, individuals will make good decisions.
Contractarianism (eg, Social contract theory)	In this context, this stipulates that businesses have a known/implied expectation and a social responsibility. The most ethical actions are those that adhere to these terms.

The school of thought held by an organization is an intrinsic part of its culture, and it will directly influence 'cyber-susceptibility' (Banks 2016; Wells & Spinks 1996). Both through the choice of defences, but also though the human factor – the daily decisions made by individuals within the organization (Rahman et al. 2021).

Method

This report has been prepared explicitly using peer reviewed articles. Business ethics and cybersecurity have been subject to significant research and it would be a wasted opportunity to use anything less than primary resources vetted through peer review.

Findings

Ironically, it was found that there is very little literature specifically considering the influence schools of thought have on cybersecurity. Below a discussion of the topic has been provided after extensive research of the available, or relevant, literature.

Discussion

Some examples of the types of human factors that leave companies susceptible to cyber-attack include social influences, attitudes to cyber-hygiene, experience/skillsets, perception of risk, and perceived cost (Rahman et al. 2021). While variability is expected between people because of personality, the choices people make will tend to align with the expectations of the

culture in the organization (Murphy & Reeves 2019). Unless there is someone monitoring mindsets, micro-managing behaviour, or setting an example with a high degree of success, it is unlikely that all employees will follow, let alone read, all the IT policies (assuming the policies contain sound advice in a legible format in the first place). An organizations culture promotes a certain type of behaviour or mindset, what that is exactly depends on the ethical frameworks in place. Therefore, culture itself can offer some defence.

An extensive review of culture is outside the scope of this report, instead an inspection of a few broad schools of thought present in many cultures and their impact on cybersecurity will be provided with some insights after extensive research.

Consequentialism

An organization that maintains a consequentialist approach is focussed on reaching positive outcomes, regardless of the means (Herschel & Miori 2017). Often the goals of organizations are not focussed on cybersecurity. While consequentialists are well meaning, they can inadvertently produce security issues as they attempt to bypass protections or grant access to an insecure third party to complete a task.

Table 2: A few perceived positives and negatives of consequentialism in relation to cyber security

Potential positive cyber outcomes	**Potential negatives cyber outcomes**
- Consequentialist can be very agile and adaptable. - Consequentialists may be more efficient and flexible with resources. - More accepting of innovative technology. - As reputation supports other goals, consequentialists may focus on security to bolster customer satisfaction. - Consequentialists appreciate regulation and will seek the best outcomes.	- Skirting around cyber-defences to complete a task. - The view that cybersecurity/cyber-hygiene is an obstacle - Minimal expenditure on cyber defences if they are perceived as a hindrance to primary desires. - May cause serious harm if the outcome is deemed more important. - A short-term mindset may result in lagging cyber defences. - In the event of a cyberattack, consequentialists may feel shame and be less transparent about the event hindering future defence and brand reputation.

Deontology

An organization that prescribes a deontological approach has rules or a code of ethics, perhaps implied in their ICT policies and mission statement, that guides their decision (Prabhumoye et al. 2020). If the organization has a solid ICT policy and well communicated cyber-hygiene expectations, one would expect it to have good cybersecurity outcomes.

Table 3: A few perceived positives and negatives of deontology in relation to cybersecurity.

Potential positive cyber outcomes	Potential negatives cyber outcomes
- They have well defined ethical codes and expectations. - Uniformity across the organization. - Highly compliant with regulation which also bolsters reputation. - Likely to be transparent about an attack, resulting in better lines of communication. - Likely to have a Long-term mindset which may incorporate cybersecurity considerations into strategic planning and risk management.	- Tendency to follow rules rigidly hinders flexibility and adaptability when required. - Heavily focussed on meeting compliance may prevent proactive efforts. - Security policies may hinder operation or result in cumbersome overhaul of systems. - Organization may be slow to respond as new rules need to be discussed and established. - Difficulty balancing competing duties. - Less consideration taken for consequences as the focus is on taking the textbook action.

Virtue ethics

An organization with a culture leaning towards virtue ethics believes that the best course of action is reached through the pursuit of virtuous qualities and fosters these within its workforce (Herschel & Miori 2017). It contends that workers in pursuit of these qualities will naturally find the most ethical course of action for a given situation. While theoretically sound, individuals may not prioritise virtues or priorities them differently regardless of what management may attempt to cultivate. These organizations may need to have more targeted recruitment of employees.

Table 4: A few perceived positives and negatives of virtue ethics in relation to cybersecurity

Potential positive cyber outcomes	Potential negatives cyber outcomes
- Given time, organizations can reach consensus on the optimal decision. - Supports an environment where ethical behaviour is valued and encouraged. - Fluid time horizons with regards to mindset (long or short term) - Flexible, adaptable, and balanced decision-making processes. - May be more proactive about cybersecurity. - Tend to generate ethical reputations.	- Subjectivity and priority of virtues makes it difficult to provide guidelines or optimal responses. - Inconsistency of ethical standards can result in confusion around security practices. - Slow to reach agreement in evolving situations. - Dependence on individuals. Also makes cybersecurity appear to be a personal issue. - May not prioritize compliance.

Contractarianism

Organizations with a culture of contractarianism accept a responsibility to society and make balanced decisions to meet this responsibility (Herschel & Miori 2017). This school of thought is becoming more common as regulation and societal repercussions have a more severe and longer lasting impact. While many organizations acknowledge a responsibility, the culture does not provide their workforce with the opportunity to act accordingly.

Table 5: A few perceived positives and negatives of contractarianism in relation to cybersecurity

Potential positive cyber outcomes	Potential negatives cyber outcomes
- Given time, decisions align well with ethical principles and business goals. - Protective of the broader community. - Cyber security practises tend to benefit all stakeholders. - Tend to have a strong commitment to regulatory compliance. - Proactive behaviours such as risk assessments are frequent. - Tend to align with ethical and secure third parties. - Are ethically adaptable as norms evolve.	- A tendency to compromise may hinder security efforts. - Balancing organizational and societal interests compromises rapid response. - Negotiations may result in a lack of clarity in policy, or potentially non-compliance. - Difficulty in addressing insider threats.

Our insight

We acknowledge that it would be irresponsible to suggest that a specific school of thought is best fit for optimizing cybersecurity, as we ourselves represent one voice in what must be a debate. However, it is worthwhile knowing the positives and negatives of your organizational ethics in relation to cybersecurity behaviours. The literature supports the notion that cultures around cybersecurity are heavily influenced by those at the head of the hierarchy, and that these people often lack the experience required to be setting the example (Banks 2016; Rahman et al. 2021; Reid & Van Niekerk 2014). Transferring this culture through the business is often achieved with positive incentives or threat of unemployment (and propagated by employing those that adhere to established norms), though there is a growing understanding that a more passive approach may be more successful in the long term (Banks 2016; Murphy & Reeves 2019).

To build a robust cybersecurity culture with an appreciation for cyber-hygiene and cyber-resilience, all members of the organization must first recognise their own moral codes, the

organizations ethics, and how they align or misalign. Additionally, individuals must realize that they are part of something designed to outlast them and operate accordingly. They need to understand cybersecurity risks and how they apply to their role within the organization (Formosa, Wilson & Richards 2021). And they need to be presented with reasonable policies, rules, and actions/behaviours that have provisions for accountability as well as an unambiguous action plan to follow in the event of an attack (Banks 2016). Once this becomes the norm, organizations should consider proactive efforts to prevent future harm. In our view, waiting on regulation is negligent. Once an organization recognises there is a need for regulation or a new protection, they have a moral duty. Managing this duty will keep them ahead of cyber-attackers and bolster reputation.

It may be beneficial for the organization to be thought of as an entity sperate from all individuals. Management and employees should consider themselves to be working for something greater than themselves, that will outlast them, and that has its own views on ethics. This will hopefully give them a greater sense of purpose and respect for the needs of the entity. Reframing in this way, along with the above suggestions, will cater to the consequentialists as there is expectations and accountability. It caters to the deontologist, as there are clear rules or unquestionable implied expectations. It caters to those following virtue ethics as it allows individuals to present their view while understanding that the organization has its own view. And it caters to the contractarians as there is a social contract between them and the organization and their objectives will often align. The reality is that people come to an end while organizations can persist. By fostering a culture that holds the organization as an entity all its own instead of it simply representing a collection of individuals, the organization can treat individuals with care for the time that they have them, and in a way that enables them to respectfully present ideas. Cyber-hygiene is then viewed as a means of protecting the entity as well as the individual, and cyber-resilience holds more value. It promotes education and more ethical decisions from every level in the hierarchy as all are working for the entity and acting with its best interests in mind. The proposed culture here, while idyllic, is one that respects and protects the entity and promotes discussion and adaptability. From a cybersecurity perspective, it promotes the idea of a human firewall.

Conclusion

Business is a survival game. People, policies, and resources ought to be managed in ways that result in the best chance of the entity persisting. Cybersecurity and reputation are two assets that require ongoing attention and, when supported properly, create great benefit. Organizational culture, and the role of individuals in the organization, must be carefully considered and maintained to ensure that the entity can stay in the game. One such culture has been present in this report.

References

Banks, N 2016, 'Practise what you preach', *Computer Fraud & Security*, vol. 2016, no. 4, 2016/04/01/, pp. 5-8.

Formosa, P, Wilson, M & Richards, D 2021, 'A principlist framework for cybersecurity ethics', *Computers & Security*, vol. 109, p. 102382.

Herschel, R & Miori, VM 2017, 'Ethics & Big Data', *Technology in Society*, vol. 49, pp. 31-36.

Hoofnagle, CJ, Van Der Sloot, B & Borgesius, FZ 2019, 'The European Union general data protection regulation: what it is and what it means', *Information & Communications Technology Law*, vol. 28, no. 1, pp. 65-98.

Jurkiewicz, CL 2018, 'Big Data, Big Concerns: Ethics in the Digital Age', *Public Integrity*, vol. 20, no. sup1, pp. S46-S59.

Line, ND, Dogru, T, El-Manstrly, D, Buoye, A, Malthouse, E & Kandampully, J 2020, 'Control, use and ownership of big data: A reciprocal view of customer big data value in the hospitality and tourism industry', *Tourism Management*, vol. 80, p. 104106.

Mantelero, A 2021, 'The future of data protection: Gold standard vs. global standard', *Computer Law & Security Review*, vol. 40, 2021/04/01/, p. 105500.

Mittelstadt, BD, Allo, P, Taddeo, M, Wachter, S & Floridi, L 2016, 'The ethics of algorithms: Mapping the debate', *Big Data & Society*, vol. 3, no. 2, p. 205395171667967.

Murphy, MC & Reeves, SL 2019, 'Personal and organizational mindsets at work', *Research in Organizational Behavior*, vol. 39, 2019/01/01/, p. 100121.

Prabhumoye, S, Boldt, B, Salakhutdinov, R & Alan 2020, 'Case Study: Deontological Ethics in NLP', *arXiv pre-print server*, 2020-10-09.

Rahman, T, Rohan, R, Pal, D & Kanthamanon, P 2021, 'Human factors in cybersecurity: a scoping review', in *The 12th International Conference on Advances in Information Technology,* pp. 1-11.

Reid, R & Van Niekerk, J 2014, 'From information security to cyber security cultures', in IEEE, Johannesburg, South Africa.

Sharif, MM & Ghodoosi, F 2022, 'The Ethics of Blockchain in Organizations', *Journal of Business Ethics*, vol. 178, no. 4, pp. 1009-1025.

Sims, RR & Brinkmann, J 2003, 'Enron Ethics (Or: Culture Matters More than Codes)', *Journal of Business Ethics*, vol. 45, no. 3, pp. 243-256.

Škanata, D 2020, 'Improving Cyber Security with Resilience', *Annals of Disaster Risk Sciences*, vol. 3, no. 1, pp. 1-10.

Warner, M 2012, 'Cybersecurity: A Pre-history', *Intelligence and National Security*, vol. 27, no. 5, pp. 781-799.

Wells, B & Spinks, N 1996, 'Ethics must be communicated from the top down!', *Career development international*, vol. 1, no. 7, pp. 28-30.

White, G & Ariyachandra, T 2016, 'Big Data and ethics: examining the grey areas of big data analytics', *Issues in Information Systems*, vol. 17, no. 4, pp. 1-7.