Cybersecurity Ethics, Professional Conduct, and Governance: Building Trust Beyond Technology

By Ismael Ifetayo Akinrinmade

Introduction

Cybersecurity is increasingly recognised not just as a technical discipline, but as a profession built on trust, responsibility, and ethical decision-making. The importance of the integrity of professionals is significant because they are entrusted with safeguarding large volumes of personal and organisational information. Cybersecurity encompasses several dimensions: Governance, Technical, and Physical protection on an international scale.

Governing bodies such as ISC2 & ISO set standards to ensure professionals adhere to certain criteria. My interest in governance stems from understanding the delicate economic, political and commercial aspects of the industry landscape. Cybersecurity begins with a top-down implementation of policies and standards from management.

Ethics in Cybersecurity: Responsibility Beyond the Law

Cybersecurity professionals often hold significant access to systems and data, which creates ethical responsibilities that extend beyond simply following the law. IT professionals often have privileged accounts across networks, systems, and data to fulfil their duties. This highlights the importance of ethical responsibility, as professionals should only use sensitive data to complete authorised tasks, while ensuring the principles of the CIA triad are maintained, and relevant laws and regulations are followed.

However, there is a clear difference between legal compliance and ethical responsibility. ISC2 highlights this distinction within its training programmes, particularly in areas such as acting ethically in the workplace, holding colleagues accountable, and upholding professional standards. Integrity is especially important when there is little or no direct oversight of privileged users, as their decisions can impact personal data, organisational assets, public trust, and wider society.

Professional Conduct and Industry Standards (ISC2 & ISO)

Professional conduct in cybersecurity is shaped by recognised standards and ethical frameworks that exist to ensure consistency, accountability, and trust across the industry.

Cybersecurity governance focuses on oversight and accountability, ensuring that security decisions are aligned with organisational objectives and managed through risk-based approaches. Professional conduct consists of performing duties in accordance with defined standards, procedures, and policies, while consistently acting with integrity, competence, and accountability. Organisations such as ISO and ISC2 provide blueprints that outline expectations for cybersecurity professionals.

The purpose of **ISO/IEC 27001** is to establish an Information Security Management System (ISMS) and to manage risk in a structured and consistent way. **ISO/IEC 27002** provides best-practice security controls that support the practical implementation of security policies across various industries and organisations. Professional bodies outline standards that can be referenced as controls or countermeasures against identified risks, which represent a form of governance within the sector through policy development.

These standards support organisations by maintaining consistency across organisational departments, enabling accountability and audit processes, and building trust with stakeholders and investors. Failing to adhere to standards and exhibiting poor professional conduct can lead to reputational damage, legal consequences, and a loss of trust and credibility.

Governance inspires me to expand my knowledge so that I can use my experience to continuously improve existing standards and contribute to the development of new ones as tools and technologies evolve within the cybersecurity community. It also shapes my professional practice when acting on behalf of others, as adhering to recognised standards is essential not only for delivering high-quality security outcomes, but also for protecting myself legally by using established benchmarks for ethical and compliant work.

Governance and Risk-Based Decision Making

Cybersecurity governance is defined as follows:

“Cyber security governance is how you control and direct your organisation's approach to cyber security. When done well, it will effectively coordinate the activities of your organisation; when done badly, it will lead to poor and delayed cybersecurity risk decision-making. Good cyber security governance enables the flow of cyber security information and decisions around the whole of your organisation.”

I like this definition by the NCSC as it highlights how governance lays the foundation for successful practices that allow organisations to securely and efficiently control the movement and use of private data. This includes meeting requirements from regulations in different countries and unions, such as GDPR and HIPAA. Governance is, however, limited to oversight, policy, and decision-making, in contrast to the technical implementation of security controls.

Risk management is a core concept of cybersecurity practice, involving the analysis of vulnerabilities and risks, and the development of strategies to minimise them while aligning with legal requirements, business objectives, and the operational costs of controls. Systems such as likelihood matrices bring harmony between technical and managerial staff by providing decision-makers with the information they need to govern the organisation, thereby supporting proactive measures that focus on long-term risk reduction rather than reacting to incidents.

My background in business studies has been a catalyst for my understanding of the contrasting goals between business objectives and cybersecurity requirements.

Social Responsibility and Public Trust

Cybersecurity incidents have real-world consequences for individuals and communities, making social responsibility a key part of professional practice in the field. Malicious activity online, ranging from network intruders (hackers) to professionals misusing their skills to cause harm, can impact individuals through violations of privacy, financial harm, and emotional stress. National Cyber Security Centre (NCSC) reported handling approximately four "nationally significant" cyberattacks per week in the year leading up to September 2025, representing a sharp increase in serious incidents.

Incidents such as fraud and unauthorised access are steadily rising as 2026 approaches, with notable attacks affecting organisations such as Marks & Spencer and Jaguar Land Rover. Incidents on this scale affect large numbers of people, causing distress and contributing to a loss of trust in public institutions such as banks and online platforms. Social responsibility, therefore, extends to cybersecurity professionals, who must protect personal data, critical services, and public confidence. Maintaining public trust when handling private data is essential, and transparency and honesty during cyber incidents are crucial. Admitting wrongdoing or mistakes, although difficult, reflects ethical responsibility and helps minimise harm while acting in the public interest.

Recent events motivate me to hold both myself and colleagues to higher professional standards, as cyber intrusions are becoming increasingly frequent and more damaging.

Personal Reflection and Career Development

Through my studies in cybersecurity, my understanding of the field has developed beyond technical problem-solving towards a broader appreciation of ethics, professionalism, and governance. My degree has exposed me to the wider responsibilities associated with protecting information systems, including accountability, risk management, and the societal impact of security decisions. This academic foundation has shaped how I view cybersecurity as a profession that requires sound judgment and ethical awareness alongside technical competence.

This perspective was further reinforced through participation in the **ISC2 Certified in Cybersecurity (CC) training course**, which emphasised ethical conduct, professional responsibility, and governance principles. My background in business studies has also strengthened my interest in governance, particularly in balancing risk, cost, and organisational objectives. Looking ahead, I aim to continue developing my knowledge in cybersecurity governance and consultancy, applying ethical principles to support informed decision-making and long-term security outcomes.

Conclusion: Trust as the Core of Cybersecurity

Ultimately, trust remains at the centre of effective cybersecurity, supported by ethical behaviour, professional standards, and strong governance structures.

In conclusion, cybersecurity is fundamentally a trust-based profession that requires ethical behaviour, professional conduct, and effective governance alongside technical expertise. Adherence to recognised standards and frameworks helps maintain accountability, consistency, and public confidence in an increasingly digital society. As cyber threats continue to evolve, the responsibility of cybersecurity professionals to act ethically and in the public interest becomes increasingly important. By prioritising governance, risk-based decision-making, and continuous development, professionals can help build secure and resilient organisations while maintaining public trust.

Refences

ISC2 (2025) *ISC2 Code of Ethics*. Available at: https://www.isc2.org/ethics (Accessed: 30 December 2025).

ISO (2022) *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. International Organization for Standardization. Available at: https://www.iso.org/standard/27001.html (Accessed: 30 December 2025).