Cybersecurity in Business: Legal, Social, Ethical, and Security Aspects

Aayan Naeem

IT-104-DL1

September 9, 2025

By placing this statement on my webpage, I certify that I have read and understand the GMU Honor Code on https://academicstandards.gmu.edu/wp-content/uploads/2023/08/George-Mason-University-Honor-Code-2023-2024-final-version-SaveasPDF.pdf and as stated, I as student member of the George Mason University community pledge not to cheat, plagiarize, steal, or lie in matters related to academic work. In addition, I have received permission from the copyright holder for any copyrighted material that is displayed on my site. This includes quoting extensive amounts of text, any material copied directly from a web page and graphics/pictures that are copyrighted. This project or subject material has not been used in another class by me or any other student. Finally, I certify that this site is not for commercial purposes, which is a violation of the George Mason Responsible Use of Computing (RUC) Policy posted on http://copyright.gmu.edu/?page_id=301 web site.

Introduction

In the digital world we have evolved into, cybersecurity has become an important part of business operation. Organizations utilize information systems to store confidential data, process transactions, simulate markets, and offer services to customers via global networks. Although such use of digital resources enables unprecedented efficiency, reach, and innovation, it also enables unprecedented risk. A single event can destabilize millions of discrete records, collapse supply chains, or annihilate public trust overnight. Reports by industry always place ranking cyber risk among the foremost risks to global economic and social stability (World Economic Forum, 2022). The business relevance of cybersecurity is far more extensive than firewalls and encryption techniques. Companies need to be entangled with overlapping compliance mandates (e.g., the US HIPAA and the EU General Data Protection Regulation), deal with ethical concerns around data collection and surveillance, and comprehend the social effects of breaches that permeate communities. Incidents such as the 2017 Equifax breach and the 2021 Colonial Pipeline ransomware attack demonstrate how cybersecurity breaches can harm consumers, employees, investors, and the public interest writ large—beyond any single company's boundary. This essay explores how achieving long-term success in the field of information technology requires a company-wide approach to cybersecurity. Technical controls alone are insufficient; organizations must blend technology decisions with legal compliance, ethical stewardship, and social responsibility. To make that case, the analysis proceeds in five stages: a technological overview of current trends and their economic benefits; examination of legal, ethical, and social issues; examination of security risks and countermeasures; and final synthesis bringing back again why cybersecurity enables organizational trust, resilience, and competitiveness.

Cybersecurity in Business: Technology Overview

Zero-trust architecture (ZTA) is a security rethink of foundational enterprise elements. Traditional, perimeter-based models implicitly trusted users and devices once they were ‘inside’ the network. ZTA rejects this assumption with the principle of “never trust, always verify.” All communications, devices, workloads, and users must be authenticated and authorized continuously, with access limited to the least privilege necessary. For organizations that enable hybrid and remote workers, ZTA reduces the risk of a single stolen credential offering unlimited lateral access. From an operational standpoint, ZTA typically unifies strong identity and access management, multi-factor authentication, device health attestation, micro segmentation, and continuous monitoring. Healthcare and financial services companies report they see measurable reductions in breach blast radius once they deploy ZTA because they can no longer easily pivot across systems once a foothold is gained.

Cloud computing transformed the manner in which businesses provision infrastructure and applications using on-demand scalability, faster deployments, and lower capital costs. But new risk comes from making the move to the public cloud. Unconfigured storage buckets, privileged identity roles, and unpatched virtual machines have led to many high-profile breaches. The shared responsibility model gives cloud providers as they are the people who look over the physical data centers and platform services, while customers are accountable for securing their data, identities, and workload configurations. Practically, this would need the use of cloud security posture management to detect misconfigurations, enforcing least-privilege access through role-based policies, encrypting data in transit and at rest, and automating patching. For example, the 2019 Capital One breach. This event serves as a reminder that cloud convenience doesn’t eliminate the need for rigorous security engineering.

IoT and OT devices offer end-to-end visibility and automation of factories, logistics facilities, retail stores, and smart offices. Sensors can anticipate the failure of equipment, prevent wastage, and optimize energy usage. These embedded systems have most of them pre-configured with insecure defaults, lack a secure update mechanism, and are in the field for years and never patched. In 2016, the Mirai botnet assaulted with hundreds of thousands of inadequately secured cameras and routers to carry out gargantuan DDoS attacks, which were manifestations of systemic vulnerabilities. In manufacturing and the utility industry, where physical processes are controlled by OT networks, separation from IT networks must be ensured. Best practices include device inventory and attestation, certificate-based authentication, network segmentation by industrial firewalls, and over-the-air (OTA) secure upgrades. Economically, IoT productivity gains are real as the spillovers of pervasive, long-term exposures should governance and lifecycle management lag adoption.

AI/ML are now a part of the mainstream security operations centers (SOCs). Anomaly detection occurs through behavioral analytics on identity activity, endpoint telemetry, and network flows; email protection leverages ML to classify phishing and business email compromise (BEC); and automated playbooks accelerate response to standard alerts. Well-calibrated, these tools reduce mean time to detect and respond. But the attackers apply AI with the same aggressiveness: generative models generate very realistic spear-phishing emails in bulk; deepfakes impersonate executive voices; and adversarial ML attempts to disable detection systems by poisoning training sets or generating inputs that classifiers sidestep. AI security then needs model control, bias testing, and human-in-the-loop validation to ensure that algorithmic pace is not bought at the expense of reliability or equity (Hu, Salcic, Zhang, & Zhang, 2021).

Compromised passwords are the source of a tremendous majority of breaches. Strong identity controls—password-less auth, hardware-based keys, adaptive risk, and conditional access—break account takeover by a huge percentage point. Privileged access management (PAM) vaults deal with admin passwords, offer just-in-time elevation, and watch sessions activity. From a business perspective, the controls protect crown-jewel systems (ERP, CRM, data lakes) and make audits easy to ensure that regulations and industry compliance are in effect. As data volumes detonate, defense needs to be designed in segregate data, decrease collection, implement tokenization and format-preserving encryption, and apply privacy-enhancing technologies such as differential privacy or secure multiparty computation for analysis against sensitive data sets. Data loss prevention solutions look over channels such as emails, webs, and cloud sync and look to see if they see anything suspicious and need to intervene by using a block exfiltration. These steps reduce the breach impacts and make it easier to abide with the law by reducing personally identifiable information and trade secret exposure.

Outside of cryptocurrency, permission blockchains build supply-chain traceability, digital identity, and notarization applications in addition to the tamper-evident ledgers. Retailers use blockchain to track food origin in seconds, closing investigation windows during recalls. In identity, decentralized identifiers (DIDs) let users prove attributes without over-sharing raw data. Adoption challenges remain—interoperability, governance, and throughput—but the security properties of immutability and distributed consensus can reduce fraud and disputes in multiparty workflows.

Although large-scale quantum computers are not yet practical for breaking today's public-key cryptography, prudent organizations are inventorying where RSA and elliptic-curve cryptography protect data with long confidentiality lifetimes (e.g., health records, intellectual property). NIST’s post-quantum standardization effort and hybrid key-establishment approaches allow businesses to begin migrating gradually, avoiding ‘harvest-now, decrypt-later’ risks. Early planning helps firms avoid a rushed, error-prone crypto migration once quantum capabilities mature.

Prevention will never be perfect. But the cyber-resilient design anticipates attacks will occur and focuses on detection, response, and recovery upfront. NIST Cybersecurity Framework which focuses on identifying, protecting, detecting, responding, and recovering, has a reproducible process. Immutable backups, disaster-recovery testing, security chaos engineering, and executive-level tabletop exercises reduce downtime when they happen. Organizations that fail early learn quicker and build customers', regulators', and partners' trust (National Institute of Standards and Technology, 2018). Another key feature of this technology is its scalability and integration properties. The majority of next-generation IT offerings have modular structures, and companies can introduce them slowly without the need to replace their existing systems. This lowers capital investment and diminishes operational disruption. For instance, cloud computing platforms and machine learning software can be added into existing processes through APIs so businesses can introduce their capabilities slowly. Scalability also makes sure that technology scales with business needs, can handle bigger sets of data, support more users, or automate more complex processes. (Zhang & Jacobsen, 2022; Gartner, 2023))

In addition, advances in security frameworks are being added directly into the technology itself. Features like real-time threat detection, automated responses, and zero-trust security architectures are becoming a normal siting in new systems. This overlap reduces dependencies and allows businesses to stay ahead of emerging cyber threats. Besides security, the technology often prefers user-oriented design allowing simple interfaces, mobile accessibility, and personalized dashboards. This not only increases adoption among employees but also supports enhanced decision-making through clearer visualization of data and insights. (Crespo-Perez, 2021)

Finally, sustainability is becoming a driving force for technology innovation. With energy efficient data centers to low-power-optimized software, there are many solutions that are being made. Not only is this saving money, but it also aligns businesses with world objectives for sustainability, which matters more to customers, investors, and regulators. Together, these aspects of scalability, embedded security, simplicity, and sustainability point us to why the technology will shake up industries and build long-term value.

Legal, Ethical, and Social Issues

Cybersecurity is under the cover of a dense body of law. In the European Union, the General Data Protection Regulation (GDPR) mandates legal grounds for processing personal data, reducing data and 72-hour notice of breach. Enforcement actions have imposed multimillion-euro fines on organizations that did not secure data or obtain lawful consent. In the United States, there is the Health Insurance Portability and Accountability Act (HIPAA), which talks about protected health information, while there is the Gramm-Leach-Bliley Act (GLBA), which goes over safeguarding customer information by financial institutions. The Consumer Privacy Act (CCPA) of California allows residents to access, deletion, and opt-out-of-sale rights to their personal information. Multinational businesses must reconcile competing duties between jurisdictions and negotiate data-transfer vehicles, especially once defining case law limited proper transfer tools. Intellectual property law intersects with cybersecurity as source code, trade secrets, and models must be guarded; a compromise that releases proprietary algorithms can disseminate competitive advantage and cause shareholder litigation.

Ethical stewardship entails more than a minimum of legal compliance. Organizations need to limit data gathering to what is necessary, inform people about purposes, and honor user expectations. AI-driven security controls must be tested for bias and explainability to ensure authentication controls or fraud models don't unfairly impact identifiable groups. Workers monitoring keystroke logging, webcam monitoring, GPS tracking can reduce insider risk but can destroy trust and productivity when applied without intent, guardrails, and proportionality. Ethical programs define principles, perform impact assessments, and implement processes to challenge or appeal automated decisions. Security breach is public: ransomware can have effects on people’s medical care, shuts down fuel pumps, or can freeze city services. Smaller businesses are in proportionally greater peril because they lack expert staff and toolsets but because they are members of big supply chains. Public-private partnership, industry information-sharing clearinghouses, and subsidized training enhance ecosystem security. The deficit in cybersecurity talent persists, expanding talent sources through community colleges, apprenticeship, and inclusive recruitment boosts capacity. Organizational culture and leadership have also been shown to contribute importantly to security behavior and success, a testament to the social nature of effective cybersecurity (Bada, Sasse, & Nurse, 2019; Crespo-Pérez, 2021; Failla, 2020; Triplett, 2022). Aside from law and ethics, the social side of cybersecurity also counts for a lot. Incidents don't stay inside corporate firewalls long; they radiate outward, undermining community confidence and outright harming citizens depending on critical infrastructure. Society meanwhile is faced with expanding digital divides—some communities and small businesses have no access to the advanced protections or awareness education that larger businesses enjoy. The lack of cybersecurity personnel only adds to the problem, leaving the majority of communities less than completely covered. Expanding talent pipelines through community colleges, apprenticeships, and inclusion-focused recruitment practices not only fills the skills gap but also creates new career opportunities. Organizational culture and leadership also have been demonstrated to contribute heavily in security behavior and effectiveness, testament to the social nature of effective cybersecurity. Collectively, these legal, ethical, and social matters demonstrate that cybersecurity is not only a technical concern but an all-encompassing societal issue that requires cooperation, transparency, and accountability on every level. (Bada, Sasse, & Nurse, 2019; Crespo-Pérez, 2021; Failla, 2020; Triplett, 2022)

Security Aspects and Challenges

The contemporary threat landscape is commercialized, dynamic, and multidimensional. Ransomware syndicates are service networks that lease affiliates toolkits containing exploits, encryption modules, and payment gateways. Double-extortion tactics—encrypting data along with the threat to release it—are used to pressure victims into paying. Downtime disruption and reputational impact normally exceed the ransom. The Colonial Pipeline attack showed how a single breach can trigger local economic effects, and this highlights the need for segmentation between operational technology and IT networks and for experienced restoration policies.

Social engineering and phishing are known to be the most common ways to gaining initial access today. Attackers exploit curiosity, urgency, authority, and fear to get clicks and credentials. Security awareness must develop from annual lectures to continuous, context-specific coaching embedded in tools. For example, there are banners that warn people about when emails originate from outside the organization. Simulated phishing can help, but programs are most successful when they do not shame and focus on positive behavioral change instead (Bada, Sasse, & Nurse, 2019).

Third-party and supply-chain risk became more prominent after events like SolarWinds, where it was demonstrated that intruding on a widely used software update had ripple effects among thousands of organizations. Good vendors of programs inventory, critically tier them, require security controls through contractual agreements, and do continuous monitoring by either shared attestation or technical telemetry. Within the firm, software bills of materials help monitor vulnerable pieces and speed patching when new vulnerabilities are publicly disclosed.

Cloud-specific risks include public exposure of storage buckets, excessively permissive identity roles, and poor API security. Guardrails such as infrastructure-as-code with security checks, CSPM, and auto-remediation reduce configuration drift. Endpoint detection and response allow visibility through many different types of technology like laptops, servers, containers, and mobile devices. When you put these all together with centralized logging, it allows fast hunting and containment.

Whether the insider threats are malicious or accidental, they are timeless. Least-privilege access, data classification, and behavior analytics can reduce this risk without stopping productivity. When breaches do occur, mature organizations employ cross-functional teams—IT, legal, communications, privacy, HR—to contain damage and meet regulatory notification obligations. Mitigation is multi-layered: strong authentication (preferably phishing-resistant mechanisms like FIDO2 security keys), patch hygiene, encryption, network micro-segmentation, and secure software development practice (threat modeling, code review, SAST/DAST, and dependency management). Compliance with frameworks such as the NIST Cybersecurity Framework and ISO/IEC 27001 formalizes risk management and enables continuous improvement (National Institute of Standards and Technology, 2018).

Resilience processes are prioritized highest in planning: maintain unmodified, isolated replicas; regularly test for recovery; establish recovery time and point objectives (RTO/RPO); and perform executive tabletop exercises. Participation in information-sharing communities and government alerts accelerates response to emerging threats. Security is finally no longer a project but an ability—permanent, measurable, and tied to business objectives.

Conclusion

Business cybersecurity is a multi-faceted, strategic discipline that anchors trust within the digital economy. The examination here illustrates that technology innovation, which spans from zero-trust and cloud through IoT and AI, is of immense value but must be deployed with smart governance and hardened design. Legislation shapes information collection, processing, and protection; ethics compel equality, openness, and consideration of agency; and social forces keep leaders aware that security incidents have consequences that spill out into society beyond corporate borders.

In practice, successful enterprises focus on cybersecurity as a business facilitator. They invest in identity and access controls, secure their cloud environments with preventive and detective guardrails, govern AI models, and govern third-party risk as intensely as they govern internal systems. They implement standards such as the NIST CSF and ISO/IEC 27001 to normalize, and to establish a demonstration of accountability to customers and regulators. They build cultures where every worker has a clear role to play in protecting information assets—and is empowered, provided with, and trained to do so.

In the coming years, quantum-resistant cryptography, privacy-enhancing computation, and continuous control monitoring will represent the next wave of security programs. But underlying imperative remains the same: keep technical controls aligned with legal, ethical, and societal responsibilities. When organizations do this, they reduce risk, accelerate recovery when problems do arise, and support the trust customers, partners, and society place in them. Cybersecurity, in short, isn't a cost center; it's the basis for long-term success in our very connected world.

References (Annotated)

Bada, A., Sasse, M. A., & Nurse, J. R. C. (2019). Cyber security awareness campaigns: Why do they fail to change behaviour? International Journal of Human-Computer Studies, 123, 29–39. https://doi.org/10.1016/j.ijhcs.2018.11.003

Annotation: This peer-reviewed article explains why most security awareness programs fail to lead to a long-term behavior change. The authors search organizational culture, message framing, and reinforcement mechanisms and said that training must be relevant, contextual, and continuous compared to being a one-time event. Their study supports this paper's focus on the human perspective as an important layer of defense. The report also gives solid suggestions like connecting content to job roles and measuring outcomes that businesses can adapt to. Accessed September 28, 2025.

Crespo-Pérez, G. (2021). Factors that influence the cybersecurity behavior: A cross-cultural study (Order No. 22619805). ProQuest Dissertations & Theses Global. http://mutex.gmu.edu/login?url=https://www.proquest.com/dissertations-theses/factors-that-influence-cybersecurity-behavior/docview/2533371753/se-2

Annotation: This dissertation examines the way values and norms among cultures affect individual cybersecurity behavior across countries. It goes over the differences in risk awareness, authority, and power distance that affect the implementing of safe behavior. The study is relevant to multinational firms developing worldwide awareness programs and policies. It supports the social nature of cybersecurity by showing that the “best practice” can’t be universally used Accessed September 26, 2025.

Failla, R. J. (2020). The influence of organizational culture on cybersecurity governance in breached organizations (Order No. 28542526). ProQuest Dissertations & Theses Global. http://mutex.gmu.edu/login?url=https://www.proquest.com/dissertations-theses/influence-organizational-culture-on-cybersecurity/docview/2543838584/se-2

Annotation: Failla discusses the impact of tone of leadership, accountability, and communication channels on cybersecurity outcomes, particularly within organizations that have experienced breaches. The study reveals that good governance and clear ownership reduce ambiguity in the event of an incident and speed up recovery. It lends credence to this paper's argument that culture is just as important as tooling. The qualitative approach provides detailed insights for managers interested in optimizing cross-functional coordination. Accessed September 27, 2025.

Gartner. (2023). *Forecast analysis: Cloud platforms, worldwide.* Gartner Research. https://www.gartner.com/en/research

Annotation: This report goes over the trends in cloud adoption and integration. It shows how APIs and machine learning tools are used in workflows. The report supports the arguments about scalability and cost benefits which I went over in the Technology Overview. Accessed September 27, 2025.

National Institute of Standards and Technology. (2018). Framework for improving critical infrastructure cybersecurity (Version 1.1). NIST. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

Annotation: NIST Cybersecurity Framework (CSF) is a well-established reference model that groups cybersecurity activities under identify, protect, detect, respond, and recover. The author has added informative references and tiers of implementation to help firms make investment priorities. Here, the CSF is the foundation of the discussion of incident response and resilience. Its neutrality and flexibility allow it to be applied to different industries and firm sizes. Accessed September 25, 2025.

Triplett, W. J. (2022). Addressing cybersecurity leadership challenges in organizations (Order No. 30522018). ProQuest Dissertations & Theses Global.
http://mutex.gmu.edu/login?url=https://www.proquest.com/dissertations-theses/addressing-cybersecurity-leadership-challenges/docview/2816676527/se-2
Annotation: Triplett focuses on leadership concepts like governance, training, communication associated with more secure stances. Executive sponsorship and clear metrics are the emphasis in the results. This reinforces the argument in the paper that security needs to be treated as a business capability and not a function of IT. The dissertation also provides practical guidance on how to develop programs. Accessed September 23, 2025.

World Economic Forum. (2022). Global cybersecurity outlook 2022. World Economic Forum.
https://www.weforum.org/reports/global-cybersecurity-outlook-2022
Annotation: This report provides data on rising ransomware expense, the persistence of human-facilitated attacks, and the widening talent deficit. The report is beneficial in arguing based on current industry data and in describing why cybersecurity remains a core strategic risk. Accessed September 28, 2025.

Zhang, Q., & Jacobsen, H.-A. (2022). Scalability and modularity in cloud-native systems: Challenges and opportunities. *Journal of Cloud Computing, 11(1),* 1–15.

https://doi.org/10.1186/s13677-022-00293-1

Annotation: This article goes over architectures in cloud systems and how they support small additions without messing up existing infrastructure. It supports the paper’s claim that scalability and integration are key drivers for technology adoption in business. Accessed September 28, 2025.

Appendix: ChatGPT Usage in Research Paper

This appendix goes over how I used ChatGPT to support my research and writing process for my paper

Topic Development & Outline

- Helped create examples and case studies like data breaches that were later checked with credible sources and used into the paper
- Suggested outline structures that were adapted to meet the assignment rubric.

2. **Drafting Support**
   - Gave sample introductions, topic sentences, and transitions. Using that for my drafts I was able to expand on it to make it better and add my own originality and depth.
3. **Proofreading & Formatting**
   - Checked paragraphs for grammar and clarity when I was unsure.
   - Gave me the APA formatting requirements like spacing, margins, references

All ChatGPT outputs were used for support and changes, but the final analysis and conclusions are my own independent research and critical thinking.