

Automation and Artificial Intelligence

Group - 4

Automation in different sectors

- ▶ Manufacturing
- ▶ Healthcare
- ▶ Retail

Manufacturing

- ▶ Using AI-backed analytics and data to reduce unplanned downtime, enhance efficiency, product quality, and the safety of employees
- ▶ Predictive Maintenance- AI helps in enhancing asset utilization, and productivity by predicting unplanned machine and equipment breakdown
- ▶ Production Enhancement- With the help of AI engines, businesses can successfully identify underlying causes of yield losses
- ▶ Quality Enhancement- AI technologies need specialist skills and the automation that manufacturers have already adopted demand skilled workforce

Healthcare

- ▶ AI already being used to diagnose and treat diseases
- ▶ AI can be extensively used in treating cardiovascular diseases
- ▶ It assist medical professionals in diagnosing illnesses faster and, using the data collected from AI algorithms, work on finding better solutions.
- ▶ Essential for healthcare providers/radiologists/pathologists to learn and implement these technologies.

Retail

- ▶ Use of robots and AI in the retail sector is growing at a rapid pace
- ▶ According to IBM, 85% of retail and 79% of consumer products companies aim to use intelligent automation for supply chain planning by 2021
- ▶ Set to redesign the entire retail industry model and the broader value chain. This transition will result in the emergence of organizations with fewer layers and a better-skilled, and trusted workforce backed by real-time data and analytics

Security Risks and Mitigations

- ▶ Hacking, phishing, ransomware, and malware attacks become more frequent and sophisticated, the adoption of hyper-automation techniques highlight how AI and machine learning present possible solutions, and can be applied at every stage of protection - from software to infrastructure, and from devices to cloud computing.
- ▶ Data breaches can be solved by AI tools that simplify data security procedures, from discovery to classification to remediation
- ▶ Security automation is expected to reduce the cost of a data breach by playing an important role in various phases of a cyberattack, such as in data loss prevention tools (DLP), encryption, and tokenization

Legal, Social, Ethical, and Professional issues faced by information security and risk professionals

Social:

Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing

- ▶ Avoid harm
- ▶ Be honest and trustworthy
- ▶ Respect the work required to produce new ideas, inventions, creative works, and computing artifacts
- ▶ Respect privacy
- ▶ Honor confidentiality

Professional Issues:

- ▶ Maintain high standards of professional competence, conduct, and ethical practice.
- ▶ Design and implement systems that are robustly and usably secure

▶ Legal:

To minimize liabilities/reduce risks, the information security practitioner must:

- ▶ Understand current legal environment
- ▶ Stay current with laws and regulations
- ▶ Watch for new issues that emerge

References

- ▶ Anon (2018) *The code affirms an obligation of computing professionals to use their skills for the benefit of society.*, *Code of Ethics*. Available at: <https://www.acm.org/code-of-ethics> (Accessed: October 24, 2022).
- ▶ Curryer, E. (2022) Automation and AI cyber security necessary to combat threats, TechInformed. Available at: <https://techinformed.com/automation-and-ai-cyber-security-necessary-to-combat-threats/> (Accessed: October 24, 2022).
- ▶ Verma, E. (2022) How AI and automation are changing the nature of work, Simplilearn.com. Simplilearn. Available at: <https://www.simplilearn.com/how-ai-and-automation-are-changing-the-nature-of-work-article> (Accessed: October 24, 2022).

Legal, Social, Ethical, and Professional issues faced by information security and risk professionals Cont..

- ▶ Liability
- ▶ Restitution
- ▶ Due care
- ▶ Due diligence
- ▶ Jurisdiction
- ▶ Long arm jurisdiction