INFORMATION ASSURANCE

Aaron Wilson

IA

Information assurance is a methodology which follows the guidelines based on its five (5) pillars of ethical business standards. These standards are integrity, availability, authentication, confidentiality, and nonrepudiation. This is used to manage data and information systems such as computers and computer networks.

THE 5 PILLARS OF INFORMATION ASSURANCE
WEBSITE AND WEB APPLICATION

INTEGRITY	AVAILABILITY	AUTHENTICATION	CONFIDENTIALITY	NONREPUDIATION
Maintains the assurance that all information systems are protected and not exposed or tampered with	Clients or users who are in pursuit of desired information have the right to access it with knowledge of risk	Those clients or users looking for such information are justifiably who they say they are	Only authorized clients or users may view a dedicated or specific data set available to the client or user	Obligatory agreement or proof that a client or user is in fact who they are digitally

COUNTERMEASURES

ANTI-VIRUS SOFTWARE	HTTPS TLS SSL CERTIFICATES	MULTI-FACTOR AUTHENTICATION OAUTH	ROLE-BASED AUTHORIZATION	TERMS OF SERVICE TOC EULA E SIGNATURE

IA RISK TRENDS FOR 2022

Top Ten

	1 RISE OF AUTOMOTIVE HACKING	2 POTENTIAL OF ARTIFICIAL INTELLIGENCE (AI)	3 MOBILE IS THE NEW TARGET	4 DATA CLOUD VULNERABILITY	5 DATA BREACHES AS PRIME TARGET	6 IOT WITH CURRENT 5G NETWORKS	7 AUTOMATION & INTEGRATION	8 TARGETED RANSOMWARE	9 STATE-SPONSORED CYBER-WARFARE	10 INSIDER THREATS
DESCRIPTION	Both Bluetooth & Wi-Fi open vehicles up to Vulnerabilities & threats	The use of AI as a means of counter defense against virus & malware threats	Mobile banking is an increasing threat by hackers	Companies' usage of data cloud is creating is increasing data leak vulnerability	Safeguard of digital data is every major company's main priority	IoT is entering a new era where 5G networks will see more increased connectivity of IoT	The agile process is becoming the normality of a company's everyday workflow	A hacker can capture and potentially corrupt personal critical data asking for ransom in return	Every country has a vested interest in gaining superiority over all others	Sabotage by waiting for a mistake is the goal of this attack
TREND	Unknown Rise in computer-aided carjackings	Groundbreaking	Up 50% from 2019	On the rise everyday as more companies join the cloud	100% commitment to cybersecurity	Groundbreaking	Steady rise	Increased medical data attacks	Waging cyber warfare to gain defense secrets	Increasing rise in human error

SUMMARY

If you dare to navigate the data-driven world of computing, networking, and the internet, you must practice the principles of solid information assurance guidelines and cybersecurity.

References

Information assurance (IA): Definition & explanation. IT Governance. (n.d.). Retrieved February 16, 2022, from https://www.itgovernanceusa.com/information/information-assurance

Duggal, N. (2021, November 19). Top 10 cybersecurity trends to watch out for in 2022. Simplilearn.com. Retrieved February 16, 2022, from https://www.simplilearn.com/top-cybersecurity-trends-article