Cheat Sheet: Using Technology to Manage Business Information

Essential Concepts

Information Technology in Business

Information technology (IT) is essential for businesses to manage and process information, playing a crucial role in daily operations and strategic decision-making in the knowledge-based economy. Technology has significantly transformed business through mobile solutions, cloud computing, extreme customer segmentation, increased connectivity, and social media, compelling businesses to embrace and adapt to these changes or face the risk of obsolescence.

Business intelligence (BI) is a technology-driven process that analyzes data from both internal and external sources to provide useful information for decision-making, helping businesses gain a competitive advantage, identify market trends, and create new strategic opportunities.

How Businesses Use Information

Technology has made it easy for businesses to gather facts about their customers and business operations. However, data are just facts and figures in their raw form. It's not until the data are processed—i.e., converted into information—that businesses can use them to improve their operations.

Businesses collect data in five broad categories: business process data, physical-world observations, biological data, public data, and personal data. Each offers valuable insights for improving efficiency, tracking physical objects, utilizing biometric information, leveraging publicly available data, and understanding individual preferences. However, the collection of these types of data also raises debates on privacy and data rights.

Being able to collect data is central to most businesses; however, all that data needs to be stored somewhere so users can retrieve it and use it. The creation of databases—virtual warehouses where data is stored—allows businesses to take the first step in managing and using data. Since the creation of "cloud computing," businesses have been able to store their

data offsite but still access it from anywhere in the world. Businesses mine data in order to find valuable patterns and answers to questions.

Managing Information

In order to make the greatest use of data, it must be shared. In business, this means that data collected by marketing needs to be shared with other departments—finance, production, research, and development—or external partners and customers, via networks. Again, this is where businesses must make decisions about the best way to share data: through intranets, extranets, or the cloud. Each has its own set of advantages and disadvantages.

A virtual private network (VPN) extends a private network over a public network, allowing users to securely send and receive data as if they were directly connected to the private network, providing functionality, security, and management benefits while utilizing the Internet's flexibility.

Issues in Information Technology

With big data comes big responsibility. This responsibility is about keeping customer and employee data safe from the threat of cyber criminals and illicit users. Large data security breaches have become more prevalent in recent years, and businesses are constantly working to find better and more effective ways to protect their data.

The widespread collection and consolidation of personal information in electronic databases raise significant privacy concerns, as both corporations and governments have access to detailed profiles of individuals, leading to potential surveillance and misuse of data, while privacy advocates strive to protect consumer rights and restrict the sale of personal information.

Artificial Intelligence (AI) is transforming businesses by enabling machines to learn, reason, and make independent decisions, impacting sectors like customer service and supply chain management. Augmented analytics combines human intuition with advanced algorithms to automate data analysis, uncovering insights and enhancing decision-making based on big data. Ethical hacking, or penetration testing, plays a crucial role in cybersecurity by identifying vulnerabilities and protecting sensitive information from unauthorized access. Additionally, digital forensics allows for the investigation and tracking of digital evidence, safeguarding corporate data and identifying potential threats.

Career Connection: Following Up

After a job interview, there are three ways to follow up: send a thank-you note to each interviewer within a day, mentioning something specific from the interview to reinforce your interest; send a follow-up note if the decision date has passed, expressing continued interest and asking if they need additional information; and if you were not offered the job but felt the interview went well, send a feedback note to inquire about constructive feedback for future

reference. Additionally, if the organization is one you admire, communicate your continued interest and ask to be considered for future opportunities.

Glossary

artificial intelligence (AI)

the simulation of human intelligence in machines, enabling them to learn, reason, and make decisions independently

augmented analytics

use of AI and advanced algorithms to automate data preparation, exploration, and analysis

business intelligence (BI)

a technology-driven process for analyzing data and presenting useful information to help executives, managers and other end users make informed business decisions

cloud computing

performing computer tasks using services provided over the Internet

data

any character, text, word, number

data mining

the identification of patterns and knowledge from large amounts of data

data warehousing

collecting and storing data from multiple internal and external sources that will be later used in analysis

digital forensics

the process of collecting, analyzing, and preserving electronic evidence to investigate and uncover information related to cybercrimes or other digital incidents

ethical hacking

also known as penetration testing, happens when organizations give permission to professionals to hack into systems to identify vulnerabilities in computer systems, networks, and applications to prevent unauthorized access and protect sensitive information by using the same methods as criminals

enterprise resource planning systems (ERP)

technology that tracks business resources and how they are used

extranet

when outside parties are provided access to a subset of the information accessible from an organization's intranet, the intranet becomes an extranet

information

data formatted in a manner that allows it to be utilized by human beings in some significant way

information technology (IT)

includes the equipment and techniques used to manage and process information

intranet

a private network accessible only to an organization's staff

point of sale systems (POS)

technology that tracks purchases by scanning barcodes and uses that data for inventory management, loyalty programs, supplier records, bookkeeping, issuing of purchase orders, quotations and stock transfers, sales reporting and in some cases networking to distribution centers

virtual private network (VPN)

extends a private network (intranet) across a public network (Internet), and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network