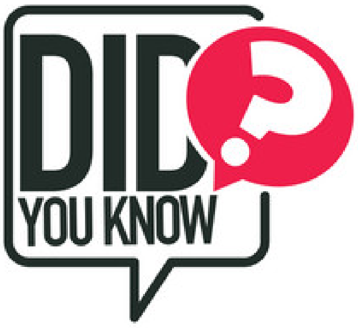


What is cognitive cyber security?

Cognitive security is the application of AI technologies patterned on human thought processes to detect threats and protect physical and digital systems. ... Such automated security systems that are designed to solve problems without requiring human resources.

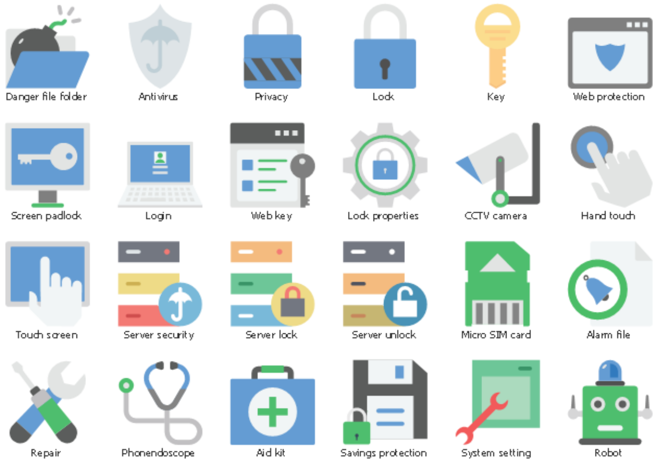
What is applied cyber security?

Applied Cyber security is a hands-on program that will give students real world security scenarios. Specialized program areas focus on database security, planning and analysis, software, and web security.

What are the elements of cyber security?

Major elements of cyber security are:

- Information security
- Network security
- Operational security
- Application security
- End-user education
- Business continuity planning



-

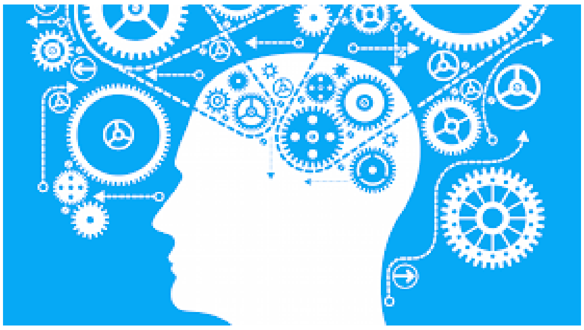
What are the advantages of cyber security?

Benefits of cyber security are as follows:

- It protects the business against ransom ware, malware, social engineering, and phishing.
- It protects end-users.
- It gives good protection for both data as well as networks.
- Increase recovery time after a breach.
- Cyber security prevents unauthorized users.

What does cognitive computing mean?

What is cognitive computing? The goal of cognitive computing is to simulate human thought processes in a computerized model. Using self-learning algorithms that use data mining, pattern recognition and natural language processing, the computer can mimic the way the human brain works.



Will cyber security be automated?

Automation can support **cyber security** professionals – but shouldn't replace them. Supported by the right tools, humans **can** do more. ... In the context of **cyber security**, artificial intelligence **can** do much of the 'legwork' at scale in processing and analyzing data, to help inform human decision making.

Is Watson a supercomputer?

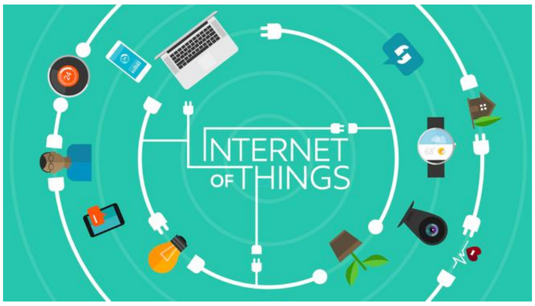
Watson is an IBM **supercomputer** that combines artificial intelligence (AI) and sophisticated analytical software for optimal performance as a "question answering" machine. The **supercomputer** is named for IBM's founder, Thomas J. **Watson**.

What is Cognitive intelligence

On the other hand, Cognitive intelligence is defined as the intellectual capabilities such as writing, reading, logic, analyzing, reason and prioritizing. Tests conducted to measure cognitive ability are used in performance analysis. Such tests are used to measure an individual's ability to solve problems in various cognitive spheres. The distinction between emotional intelligence and cognitive intelligence is evidenced in the psychometric tests of assessing cognitive ability and psychometric tests of intelligence

How Internet of Things (IoT) security become best practices

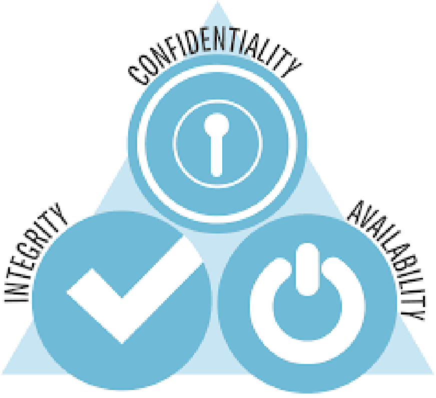
- IOT security best practices to keep in mind
- Discover what IOT actually looks like for you now, and in the future. Generate an inventory of the IoT devices you have, and how those devices can affect cyber security, privacy, and human risks.
- Make IOT an integral part of your cyber security program. What used to be a common practice of 'connect it first, secure it later' is not feasible. Conduct end-to-end cyber security risk assessments that consider IOT as part of your overall risk.



- Remember that IoT security requires a layered approach. You want to make sure your endpoint devices, their communications (wired and wireless networks and gateways), as well as their data and applications are highly secured.
- Be aware of your IoT ecosystems' risks in the physical world. Thorough IOT security assessments should ideally include the physical environment, and the risks posed to your connected devices by threats that may include humans, vehicles, biohazards, and natural disasters.

Explain CIA.

CIA stands for **Confidentiality, Integrity,** and **Availability. CIA** is a model that is designed to guide policies for Information Security. It is one of the most popular models used by organizations.



Confidentiality

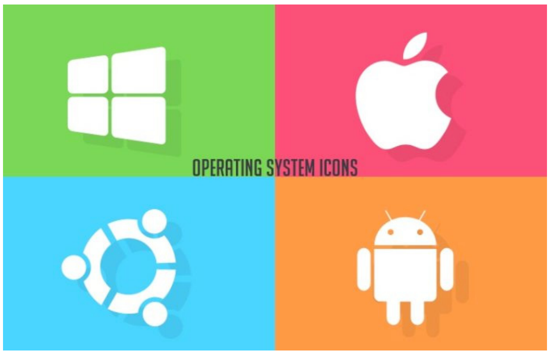
The information should be accessible and readable only to authorized personnel. It should not be accessible by unauthorized personnel. The information should be strongly encrypted just in case someone uses hacking to access the data so that even if the data is accessed, it is not readable or understandable.

Integrity

Making sure the data has not been modified by an unauthorized entity. Integrity ensures that data is not corrupted or modified by unauthorized personnel. If an authorized individual/system is trying to modify the data and the modification wasn't successful, then the data should be reversed back and should not be corrupted.

How IT starts in the OS

Security cannot be thought of as an add-on to a device, but rather as integral to the device's reliable functioning. Software security controls need to be introduced at the operating system level, take advantage of the hardware security capabilities now entering the market, and extend up through the device stack to continuously maintain the trusted computing base. Building security in at the OS level takes the onus off device designers and developers to configure systems to mitigate threats and ensure their platforms are safe.



Why is anomaly detection critical for data-driven enterprises?

Today, companies have started to understand the importance of interconnected operations. Firms rely on real-time data to get a 360 degree view of their business. However, the voluminous data and the rush of coordinated activities taking place at scale make it challenging to spot anomalies. Anomaly detection refers to the problem of finding patterns in data that don't follow expected behavior. Datasets that don't follow a pattern are termed as anomalies or outliers.

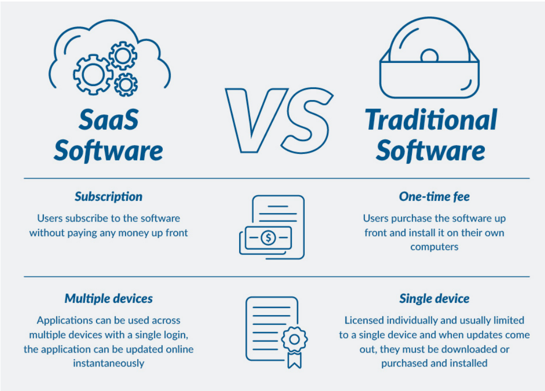
Examples of potential anomalies:

- A leaking boiler resulting in the shutting down of the entire production line
- Too many failed login attempts signaling the possibility of fishy cyber activity
- Fraud detection in financial transactions

While the possibilities of anomaly detection are limitless, a single person or a traditional analytics system cannot study massive amounts of data to spot anomalies. There is a need for scalable systems that can automate the whole process.

One of the biggest challenges for IT departments is the ability to detect and respond to critical events such as cyber attacks in real time. This problem will only compound as the amount of machine data organizations produce is expected to grow 15 times by 2020. There is simply no way traditional monitoring systems will be able to effectively manage this volume of data.

What is SaaS?

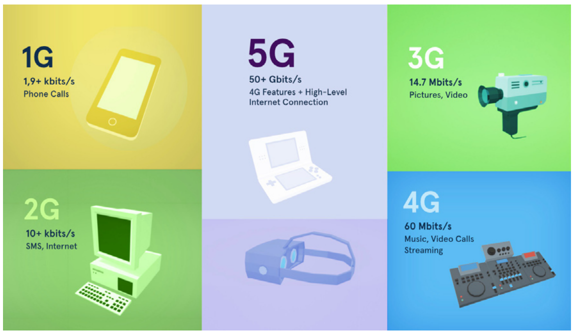


SaaS Software	VS	Traditional Software
Subscription Users subscribe to the software without paying any money up front		***One-time fee*** Users purchase the software up front and install it on their own computers
Multiple devices Applications can be used across multiple devices with a single login, the application can be updated online instantaneously		***Single device*** Licensed individually and usually limited to a single device and when updates come out, they must be downloaded or purchased and installed

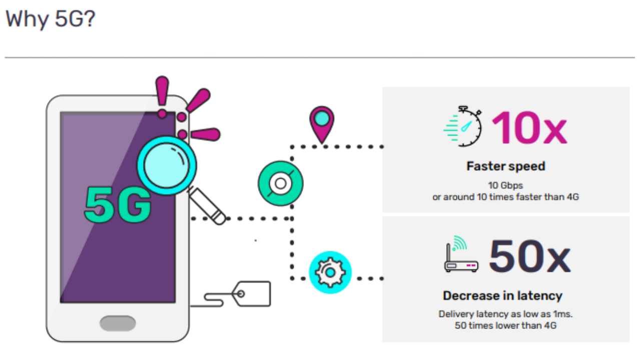
SaaS is a software distribution model that offers a lot of agility and cost-effectiveness for companies, which is why it's such a reliable option for numerous business models and industries. It's also popular amongst businesses for its simplicity and user accessibility, security, and the widespread connectivity that serves to streamline business models, resulting in maximum efficiency across the board. Today, most companies are in the process of implementing various business intelligence strategies, turning to SaaS BI tools to assist them in their efforts.

SaaS is a good starter project for IaaS and PaaS. SaaS is the most basic of the three layered models that are at the heart of the cloud provider model for organizations. The other two layers are Infrastructure as a Service (IaaS) and Platform as a Service (PaaS). While SaaS can be as small as one app, IaaS and PaaS represent seismic shifts in the way your firm does business. IaaS includes services and processes such as website hosting, big data analysis, backup, disaster recovery, provision of room for testing by developers and more. PaaS means hosting your entire platform online, allowing complete platform access with a single login.

Why 5G is Important for Enterprises



5G is an emerging technology that makes over underlying architecture in core networks and promotes virtualization, IT and automation. It changes the possibilities of networks, applications and underlying IT systems. It introduces new technologies such as edge computer and network slicing to enable the introduction and ubiquity of immersive solutions. These solutions are what will make available the tools for organizations – IT departments and lines of business – to renovate digitally and construct new business outcomes that have traditionally not been associated with IT.



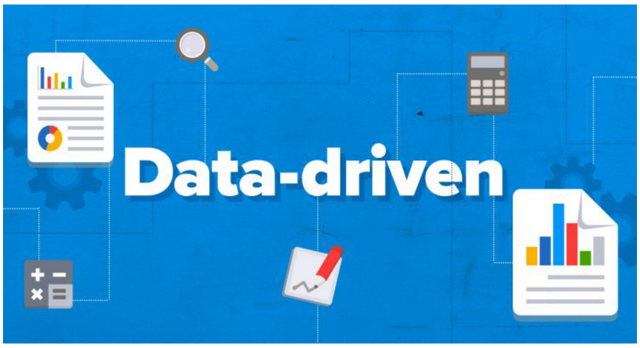
Source: https://www.infosys.com/engineering-services/insights/Documents/Infosys-thought-leadership-5g.pdf

Who are the movers of 5G technology?

Industries in transformation are the likely first movers with the adoption of 5G solutions. Manufacturers, for example, are looking at ways to interconnect people, devices and objects, merging the physical and IT systems and using the latest technologies in robotics, AI and IoT to drive innovation.

What is Data Driven Security?

Data driven security is a notion utilized by organizations operating in a continuously changing surroundings to efficiently administer the energetic risks which challenge their organization. Security professionals operating in today's increasingly aggressive environments face the inimitable confront of providing security that reduces crime and loss, is cost effective, and does not depiction their organizations to unnecessary accountability.



Data driven security is an effectual method of balancing those factors. In order to be victorious at this balancing act, security professionals must not only be knowledgeable about security, but they must also be good quality business decision makers and risk managers.