**UNIT - V**

**Security for Internet of Things:**

The Internet of Things (IoT) is a network of connected devices, each with a unique identifier that automatically collects and exchanges data over a network.

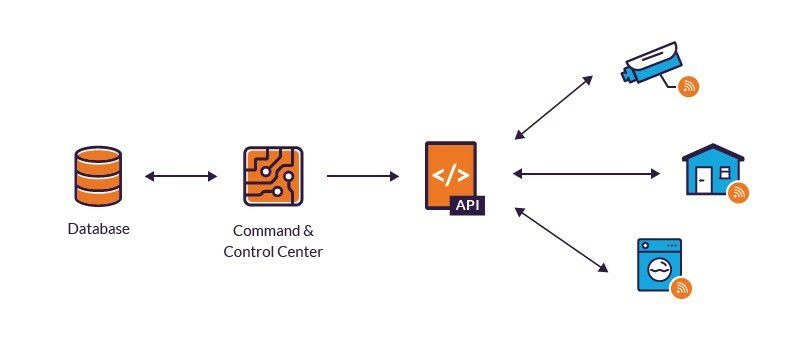
IoT devices are used in multiple sectors and industries, including:

Consumer applications – IoT consumer products include smartphones, smart watches and smart homes, which control everything from air conditioning to door locks, all from a single device.

Business applications – Businesses use a wide range of IoT devices, including smart security cameras, trackers for vehicles, ships and goods, as well as sensors that capture data about industrial machinery.

Governmental applications – Governmental IoT applications include devices used to track wildlife, monitor traffic congestion and issue natural disaster alerts.

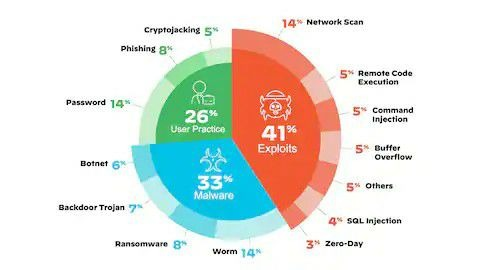
The number of IoT devices worldwide now numbers in the billions. Their increased presence in our daily lives has led to increased scrutiny of their inherent security issues, which we will be exploring here.



While relatively new as a cybersecurity discipline, the Internet of Things (IoT) as a business enabler has matured into a clearly defined set of use cases solving pressing business problems that deliver operational and cost benefits across many industries, such as healthcare, retail, financial services, utilities, transportation and manufacturing.

The rapid growth of capabilities and adoption of IoT technology has fueled a transformation in enterprise operations with IoT devices making up 30% of total devices on enterprise networks today. Rich data collected from these devices provides valuable insights that inform real-time decisions and deliver accurate predictive modeling. In addition, IoT is a key enabler of digital transformation in the enterprise, with the potential to drive up workforce productivity, business efficiency and profitability as well as the overall employee experience.

Despite the many advantages and innovations IoT technology enables, the interconnectedness of smart devices presents a substantial challenge to enterprises in terms of grave security risks arising from unmonitored and unsecured devices connected to the network.



**Understanding the risk:**

Risk is the probability of an outcome having a negative effect on people, systems or assets. Risk is typically depicted as being a function of the combined effects of hazards, the assets or people exposed to hazard and the vulnerability of those exposed element.

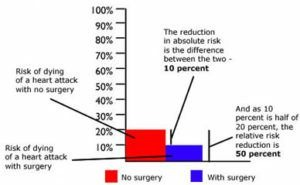
By understanding these risks, the project manager can then select strategies and implement response plans to address them. Similarly, opportunities can be identified at the planning stage of a project and should be used in areas like finance and time to help achieve a more positive outcome from the project objectives.

Types of Risks:

Widely, risks can be classified into three types: Business Risk, Non-Business Risk, and Financial Risk.

What is a risk?

You may find the following information useful to share with patients who would like to understand more about the numbers involved in interpreting the benefits and harms of treatments. You may also find some ideas about how to discuss risk with your patients.



**Getting to a bad place:**

When the internet was created and especially the web, much effort was invested into the interconnection of machines, transmission of messages, and publication of information, and little effort was made concerning the problem of how to avoid malicious users sabotaging the network and published information. Good people will not consider the fact that bad people will share the network with them. Resilience was defined as the ability to recover from faults. This would typically mean infrastructure losses and breakdowns, which were imagined to be random events, natural disasters, or wars, which were large scale local area events. Malicious attacks, however, do not affect components randomly, or locally, but systematically and globally, and in a much more sophisticated manner. Attacks exploit vulnerabilities in the design or code, to make it do things that were never intended or imagined. As such, protection mechanisms have not naturally developed. It is difficult to develop.

**Understanding the root cause:**

Root cause analysis (RCA) is the process of discovering the root causes of problems in order to identify appropriate solutions. RCA assumes that it is much more effective to systematically prevent and solve for underlying issues rather than just treating ad hoc symptoms and putting out fires.

How to Perform a Root Cause Analysis in 5 Steps?

Define the Problem.

Analyze what you see happening and identify the precise symptoms to form a problem statement.

Gather Data.

Identify Causal Factors.

Determine the Root Cause(s).

Recommend and Implement Solutions.

Step 1: Identify Possible Causal Factors.

Step 2: Identify the Root Cause.

Step 3: Identify Communication Challenges.

Step 4: Prioritize Communication Challenges.

**Root cause analysis principles:**

Root cause analysis is flexible enough to accommodate different types of industries and individual circumstances. Yet beneath this flexibility, the following four important principles are essential to making RCA work:

**1. Learn why, how and when the incident occurred**

These questions work together to provide a complete picture of the underlying causes. For example, it can be difficult to know why an event occurred if you don't know how or when it happened. Investigators must uncover an incident's full magnitude and all the key ingredients that went into making it happen at the time it happened.

**2. Focus on the underlying causes, not the symptoms**

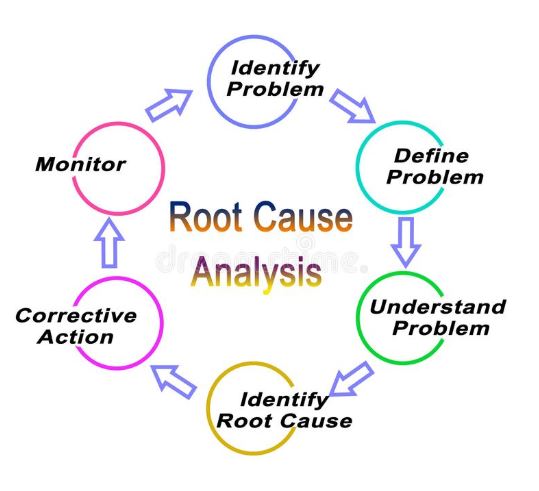
Addressing only the symptoms when a problem arises rarely prevents that problem from reoccurring, and can waste both time and resources. An RCA effort should instead focus on the relationships between events and the incident's underlying root causes. In the end, this can help reduce the time and resources spent on resolving issues and ensure a viable solution over the long term.

**3. Think prevention when using RCA to solve problems**

To be effective, an RCA effort must get to a problem's root causes -- but that's not enough. It must also make it possible to implement solutions that prevent the problem from reoccurring. If the RCA doesn't help fix the problem and keep it from happening again, much of the effort will have been wasted.

**4. Do it right the first time**

An RCA is only as successful as the effort behind it. A poorly executed RCA can waste time and resources. It might even make the situation worse, forcing investigators to start over. An effective root cause analysis must be carried out carefully and systematically. It requires the right methods and tools, as well as leadership that understands what the effort involves and fully supports it.



**Looking at alternate options:**

Datadog:

Datadog is a monitoring service for IT, Dev and Ops teams who write and run applications at scale, and want to turn the massive amounts of data produced by their apps, tools and services into actionable insight.

ArborXR:

ArborXR puts you in command of XR device management. Confidently manage VR & AR devices at scale, remotely deploy content, and control what users can see and do. ArborXR is built with enterprise-level security and in direct partnership with a number of Fortune 500 companies.

Hologram:

The easiest to use cellular platform for IoT. Connect your entire fleet anywhere, on every network, all powered from a single SIM card.

Azure IoT Hub:

Azure IoT Hub is a scalable, multi-tenant cloud platform (IoT PaaS) that includes an IoT device registry, data storage, and security. It also provides a service interface to support IoT application development.

Google Cloud IoT Core:

Google Cloud IoT Core is a fully managed service that allows users to easily and securely connect, manage, and ingest data from millions of globally dispersed devices.

Azure IoT Central:

Azure IoT Central brings the Internet of your things to life by connecting your devices, analyzing previously- untapped data, and integrate business systems and transforming your company when you uncover new business models and revenue streams.

SensorCloud:

MicroStrain’s SensorCloud™ is a unique sensor data storage, visualization and remote management platform that leverages powerful cloud computing technologies to provide excellent data scalability, rapid visualization, and user programmable analysis.

IBM Watson IoT Platform:

IBM Watson IoT Platform is a managed, cloud-hosted service designed to make it simple to derive value from your Internet of Things devices.

Exosite ExoSense IOT:

ExoSense enables users to monitor equipment status and performance, manage user and asset groups, build tailored insights and dashboards, and define alerts and notifications. Customized and deployed without the need for a software developer, ExoSense enables customers to see immediate value from the Murano platform with no coding experience required.

Azure IOT Solution Accelerators:

Use templates to create fully customizable solutions for common Internet of Things (IoT) scenarios—Bring your business together in insightful new ways from increasing process efficiencies to delivering better customer experiences and generating new revenue streams.

**Getting to better place:**

The combined effect of climate change and society’s impact on the earth is intensifying struggles over natural resources while also threatening our infrastructure, food systems and quality of life. It’s increasingly clear that today’s environmental conditions are not sustainable. Over the past few decades, we have made huge progress fighting disease, poverty and illiteracy. Now we must apply that same ingenuity to the problem of global warming and other consequences of human activity. Confronting these challenges requires political will, as well as a new approach to business--one that puts human welfare on an equal footing with profits. It also calls for innovative technology. We are already starting to see how the Internet of Things (IoT)—which connects everyday objects to the Internet—can help us transform our world for the better. Along with advanced data analytics, IoT-enabled devices and sensors are helping us reduce air pollution in some of our world’s biggest cities, improve agriculture and our food supply, and even detect and contain deadly viruses.

Smarter cities:

Cities are also great incubators for IoT-based systems that make urban life more attractive, such as fast, convenient transportation systems, safe street lighting and energy-efficient buildings.

A citywide WiFi and information network linked to sensors, software and a data analytics platform has enabled the city to provide smart water technology, automated street lighting, remote-controlled irrigation for parks and fountains, “on-demand” waste pickups, digital bus routes and smart parking meters. These IoT-enabled urban services have dramatically reduced traffic jams and pollution, as well as water, light and energy usage.

Cleaner air and water:

Drayson Technology has been testing sensors that are distributed to bicycle couriers and a fleet of fuel-cell cars. The sensors, which transmit data to smartphones via Bluetooth, allow Drayson to create real-time maps showing air pollution levels around the city.

CityVerve is developing IoT infrastructure for everything from culture, healthcare, energy and travel, making Manchester a more sustainable city while also providing a blueprint for others.

Smarter Agriculture:

From massive agribusiness players like Cargill to small organic farmers, growers all over the world are using the Internet of Things to reduce their consumption of water and fertilizers, cut waste and improve the quality or yield of their products. Examples range from tracking microclimates across cropland, to closely monitoring temperature changes and humidity levels as perishable goods move from field to warehouse to store in order to extend their shelf life and eliminate waste.

Cutting food waste:

Through a combination of advanced cameras, sensors, weather stations and artificial intelligence, Israeli startup Prospera can help farmers respond quickly to problems while also boosting productivity by as much as a third. Shrini Upadhyaya, a professor at the University of California, Davis, devised a wireless sensor system to continuously monitor leaf health, which helps farmers know exactly where and how much they need to irrigate. And throughout rural Africa, startups such as Farmerline and ArgoCenta are using mobile technology and Big Data platforms to empower smallholder farmers who need access to market data quickly in order to cut waste, improve operations and digitize their supply chains.

Connecting Patients:

The Internet of Things can transform the healthcare industry by helping doctors gain faster access to patients’ data. Wearable, Internet-connected sensor devices that track a patient’s heart rate, pulse, or even blood pressure are increasingly affordable, compact and accurate. While there is still some debate over how to safely collect, transmit and use this data, wearables are one of the most promising IoT applications in healthcare.

Increasingly, technology is also helping doctors and other medical professionals monitor the wellbeing of patients who live independently. Sensors, or even robotic assistants, can alert caretakers if patients forget to take their medicine or do not leave their bedroom by a set time.

**Mastering data protection technologies:**

Types of Master Data:

Customer data: is used to track and manage customer relationships. ...

Product data: is used to track and manage the inventory of an organization.

Financial data: is used to track and manage the financial performance of an organization.

The most commonly found categories of master data are parties (individuals and organisations, and their roles, such as customers, suppliers, employees), products, financial structures (such as ledgers and cost centers) and locational concepts.

Data protection solutions rely on technologies such as data loss prevention (DLP), storage with built-in data protection, firewalls, encryption, and endpoint protection.

However, here are 7 of the most effective data security techniques that you can try to secure your data.

Data encryption.

Backup and recovery optimization.

Data masking.

Row level security.

Promote transparency and compliance.

Cyber insurance.

Work with experts in data.

The terms data protection and data privacy are often used interchangeably, but there is an important difference between the two. Data privacy defines who has access to data, while data protection provides tools and policies to actually restrict access to the data. Compliance regulations help ensure that user’s privacy requests are carried out by companies, and companies are responsible to take measures to protect private user data.

Data protection and privacy is typically applied to personal health information (PHI) and personally identifiable information (PII). It plays a vital role in business operations, development, and finances. By protecting data, companies can prevent data breaches, damage to reputation, and can better meet regulatory requirements.

Data protection solutions rely on technologies such as data loss prevention (DLP), storage with built-in data protection, firewalls, encryption, and endpoint protection.

**Skimming basics of encryption:**

Encryption is a security control used primarily to provide confidentiality protection for data. It is a mathematical transformation to scramble data requiring protection (plaintext) into a form not easily understood by unauthorized people or machines (ciphertext).

What are the 4 basic types of encryption systems?

\*Advanced Encryption Standard (AES)

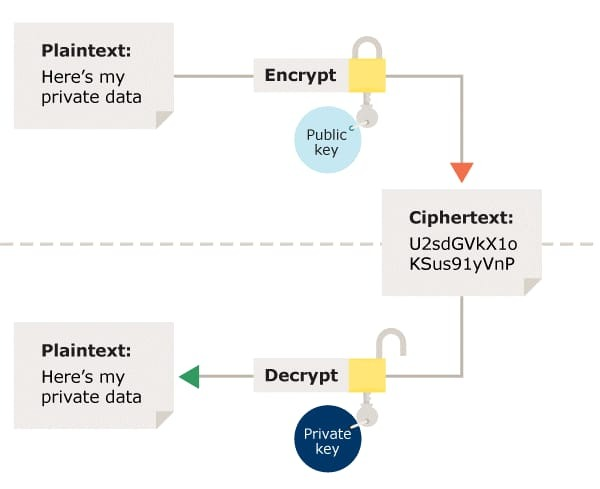
\*Triple DES.

\*Blowfish.

\*Rivest-Shamir-Adleman (RSA)

RC4, a symmetric stream cipher (i.e. the same algorithm can be used to encrypt and decrypt). RC4 no longer offers adequate security and has been deprecated in PDF 2.0.

AES (Advanced Encryption Standard) specified in the standard FIPS-197.



There are two basic methods of encryption: symmetric and asymmetric. Symmetric encryption uses the same key for encryption and decryption. Asymmetric uses a different key for encryption and decryption. A key is an external piece of information, like a password, used to cipher or decipher the code.

**Protecting data integrity:**

1.Perform Risk-Based Validation.

2.Select Appropriate System and Service Providers.

3.Audit your Audit Trails.

4.Change Control.

5.Qualify IT & Validate Systems.

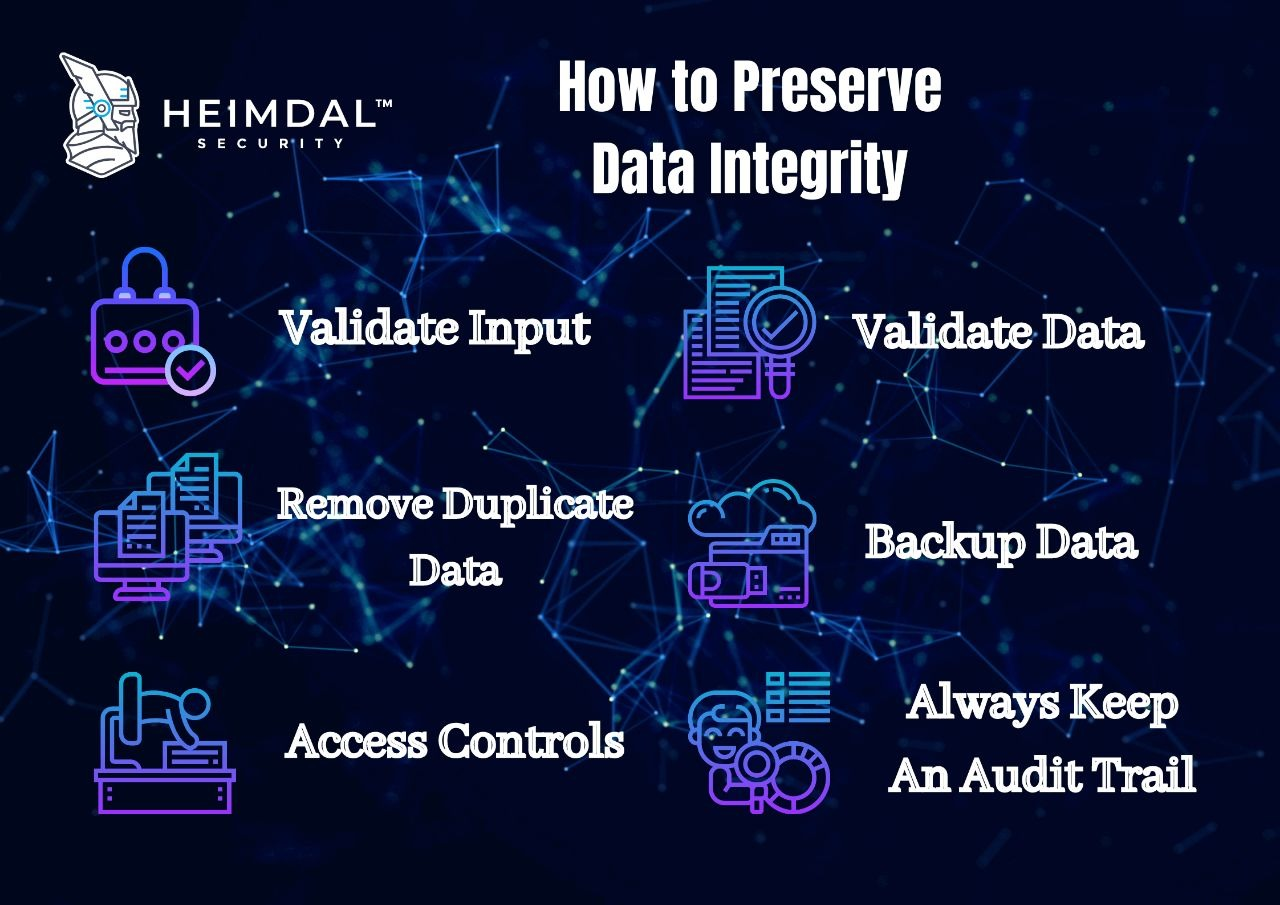
6.Plan for Business Continuity.

7.Be Accurate.

8.Archive Regularly.

The Steps for maintaining Data Integrity are:

Always Validate Input Data. Implement Access Controls. Keep an Audit Trail. Always Backup Data.



4 Simple Steps to Ensure Data Integrity in Quality Control Labs:

Data Integrity. Many data integrity issues can be traced back to human error; therefore, ensure that data integrity starts with the user.

Understand your Process Workflow and Data Lifecycle.

Automate Data Workflows.

Review Data for Quality and Completeness.

**Understanding the key sizesusing certificates:**

When you're using CloudFront alternate domain names and HTTPS, the maximum size of the public key in an SSL/TLS RSA certificate is 2048 bits. (This is the key size, not the number of characters in the public key.)

A certificate contains a public key. The certificate, in addition to containing the public key, contains additional information such as issuer, what the certificate is supposed to be used for, and other types of metadata. Typically, a certificate is itself signed by a certificate authority (CA) using CA's private key.

Go to the Security tab and click on View Certificate. You'll see three tabs on the top of the page.The first would be the website's name.

In the Public Key Info, you'll see information relating to the algorithm (in this example, it's the RSA algorithm) and the SSL key size (which is 2048 bits for digicert.com).

One of the TLS/SSL certificates used by your server uses a key that is considered weak due to its small key size. The recommended minimum sizes for RSA and ECDSA keys are 2,048 bit and 256 bit, respectively.

**Avoiding self-signed certificates:**

A. Self-configuration

The system is capable to readjust itself. Readjustment of the system is required if its environment changes or to reach an objective set for the system.

B. Self-optimization

The system can measure its current performance and it able to compare it against to the known optimum level of performance. The system will adjust its operation to reach closer the optimal performance. The system is also able to change its operation to cope with new user set policies.

C. Self-healing

The system tries to recover from faults or to avoid them. Self-healing can be implemented in two different styles. They are reactive and proactive modes. In reactive mode the system detects and recovers from faults as they occur. The system also tries to repair the faulted functions if possible. In proactive mode the system monitors its state to detect and adjust its behaviour before reaching an undesired state.

D. Self-protection

The system defends itself against internal and external threats, which can be accidental, such as cascading failures, or malicious attacks against the system. To manage the threats the system must be aware of its environment and have means to react to detected threats.

E. Self-management in wireless sensor networks

The self-management intelligence is located in the motes of the WSN. Mostly the self-management concerns the motes, however there are also some network level self-management objectives such as self-discovery and self-organization. Self-discovery means that the motes of the WSN search for services available for them automatically. An example of a service is routing in multihop networks, where the messages for and from motes out of reach of the network controller are routed through other motes that are in reach of the controller. In self-organization the motes of the WSN adjust the logical topology of the network to improve the reliability and scalability of the network.

The certificate is signed by the Issuing Certificate authority, and this it what guarantees the keys. Now when someone wants your public keys, you send them the certificate, they verify the signature on the certificate, and if it verifies, then they can trust your keys.

By successfully passing the IoT Fundamentals exam, you'll obtain the certificate that affirms your knowledge of basic IoT concepts, principles, and enabling technologies. The certificate also validates your ability to use IoT operating systems and applications.

In their simplest form, a certificate contains a public key and a name. The certificate may also contain an expiration date, the name of the certifying authority that issued the certificate, a serial number and optional additional information.

SSL/TLS certificates are used to authenticate the identity of a website and create a secure connection between the server and a browser.

Different Types of SSL Certificates:

Extended Validation (EV)

Organization Validation (OV)

Domain Validation (DV)

Other examples might include:

CFA (Chartered Financial Analyst)

CIPM (Certificate in Investment Performance Measurement)

RA (Registered Architect)

CPL (Commercial Pilot License)

CMP (Certified Meeting Professional)