

Securing IoT

Lê Thế Dũng, Ph.D.

Dep. of Computing Fundamentals, FPT University, Viet Nam

January 2024



Outlines

- Security and Privacy Implications of IoT Overview
- Security Issues Related to IoT
- Privacy and Ethics
- Cyber Security Methods
 - Authentication; Authorization; Network Enforced Policy; Secure Analytics: Visibility and Control
- Off The Shelf IoT
- Fog Computing
- Encryption
- Identifying IoT Security Risks

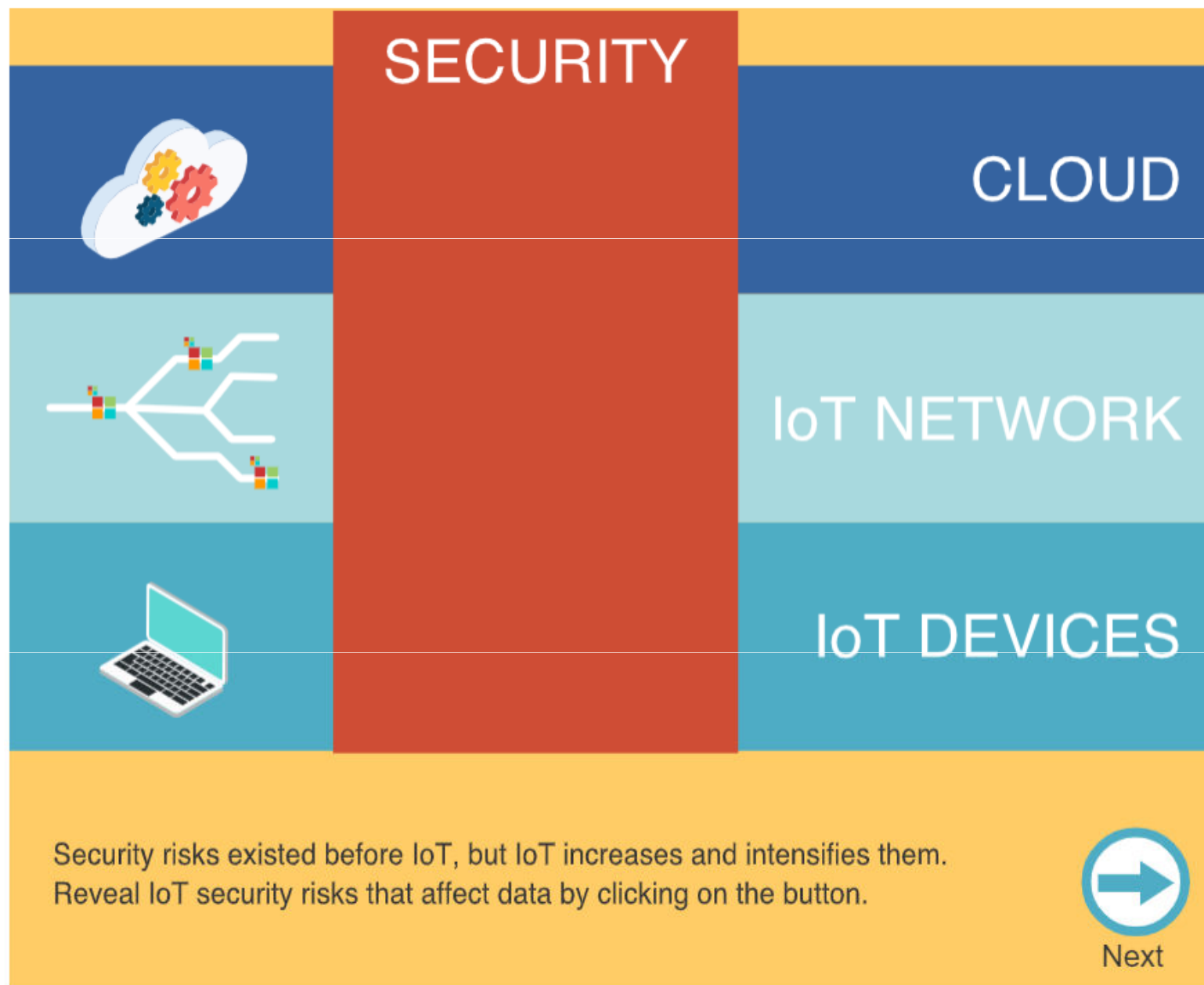
Security and Privacy Implications of IoT

- Internet of Things involves:
 - extra devices being connected
 - extra networking to connect these devices
 - extra programming to direct the devices and networking
 - a massive volume of extra data pouring into the internet
 - more machine to machine (M2M) interactions and autonomous decision making.
 - Each of these layers brings **additional security issues**.
- Securing the Internet of Things is a highly necessary and complex task that sits across the top of its devices, networks and applications, but must be considered and factored into the design and planning phase.
 - Many IoT devices are purposely very small and low powered, and this increases the difficulty of securing them.

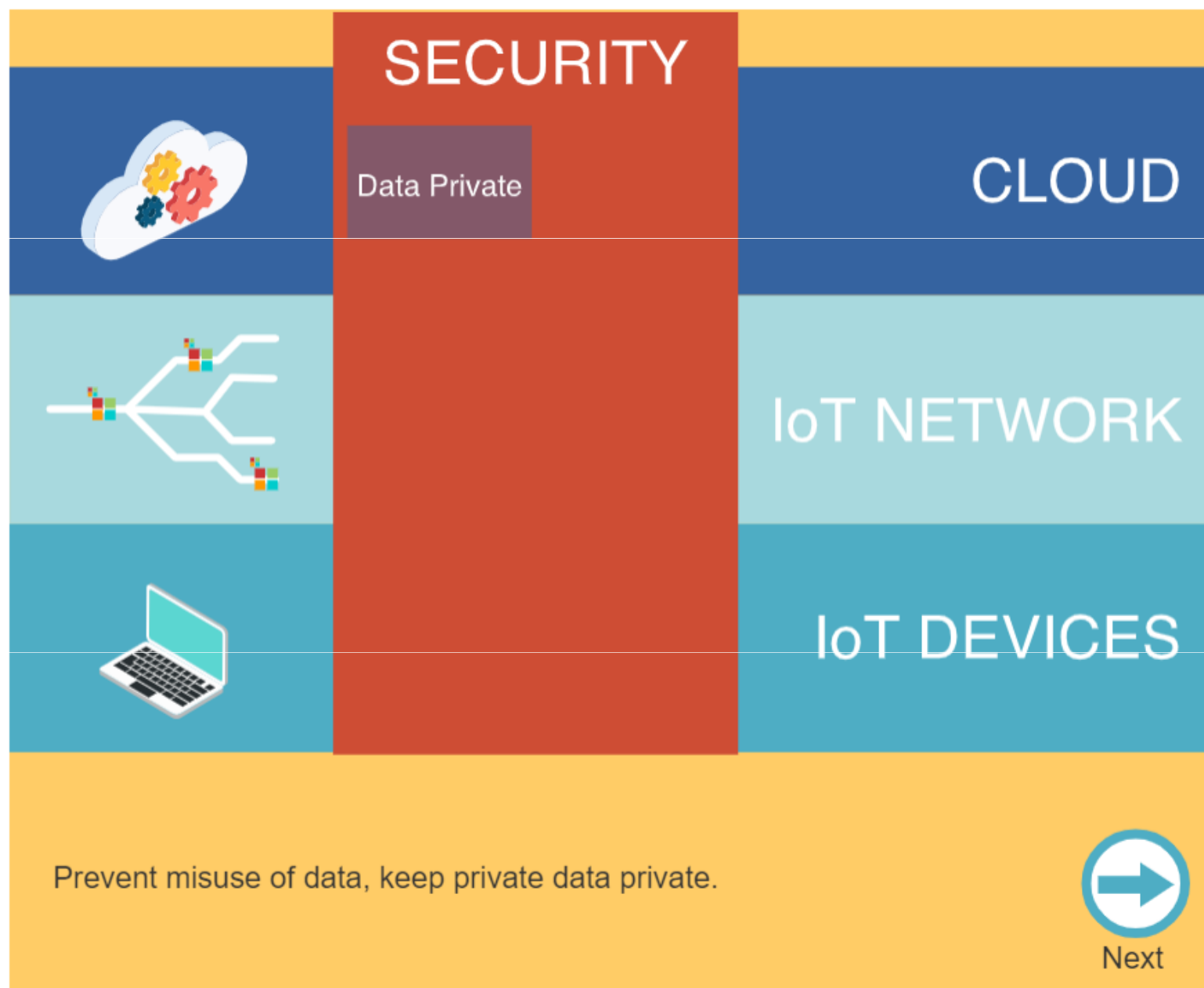
Security and Privacy Implications of IoT (cont.)

- Connecting things up makes private data about ourselves, our lives, and our businesses **accessible**. The Internet of Things challenges notions and ethics of privacy, factors which must be considered and designed for.
- There is also the concern that IoT technology development is **outpacing the governance** and regulation required, as well as the ability of many individuals to be aware of the threats and know how to address them.
- Aside from digital security risks, we also need to know how to keep IoT devices **physically secure**.

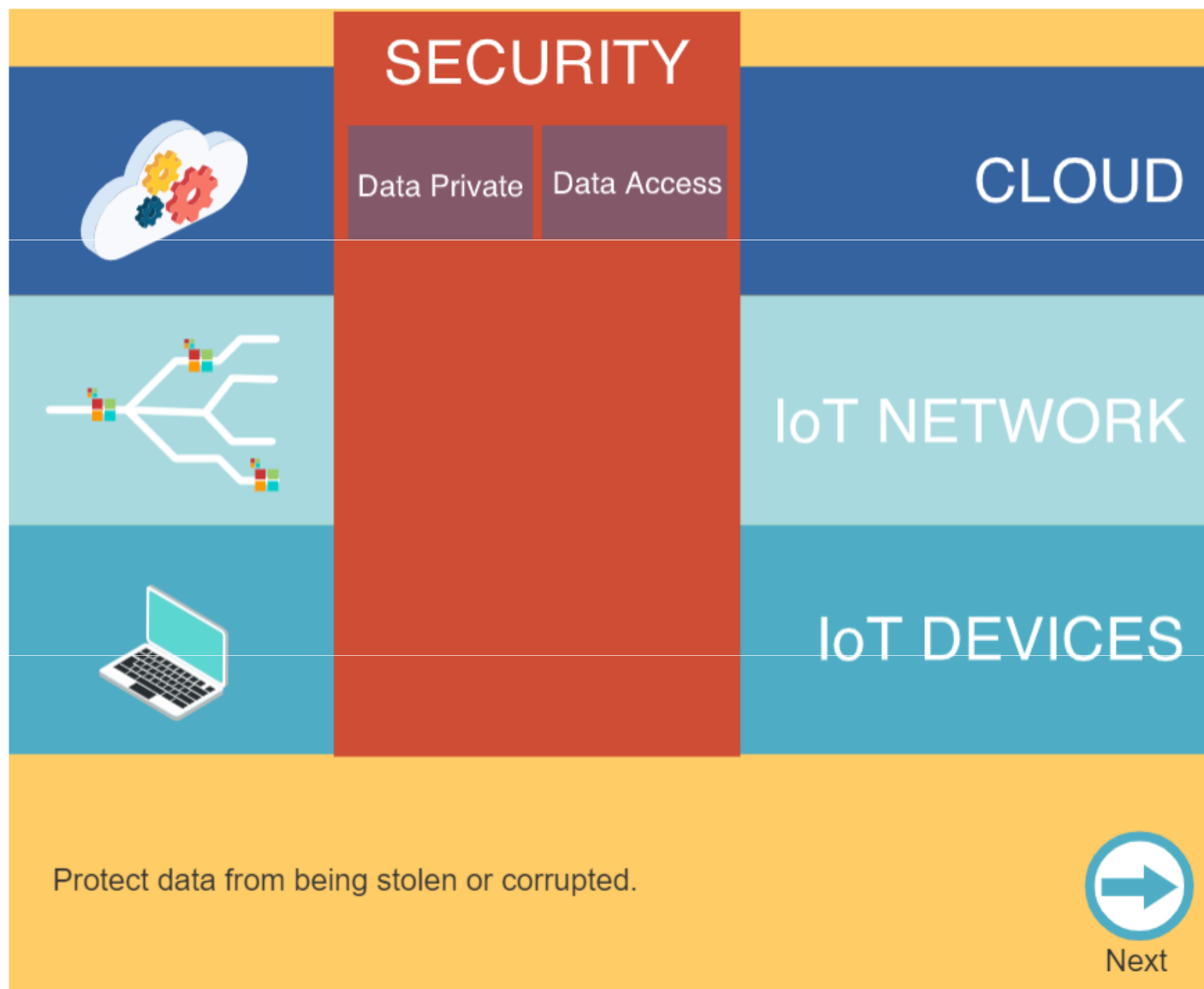
Security Issues Related to IoT



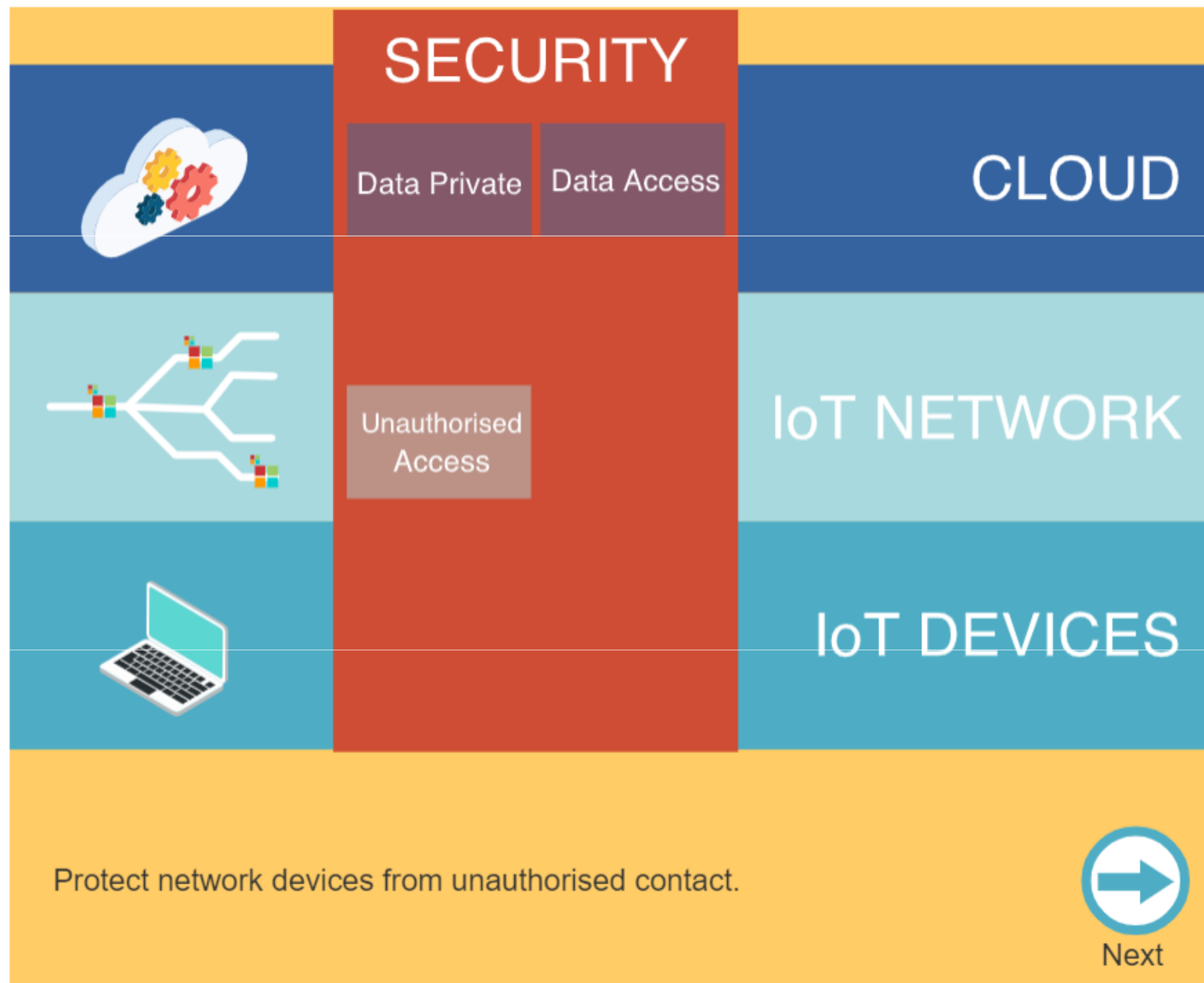
Security Issues Related to IoT (cont.)



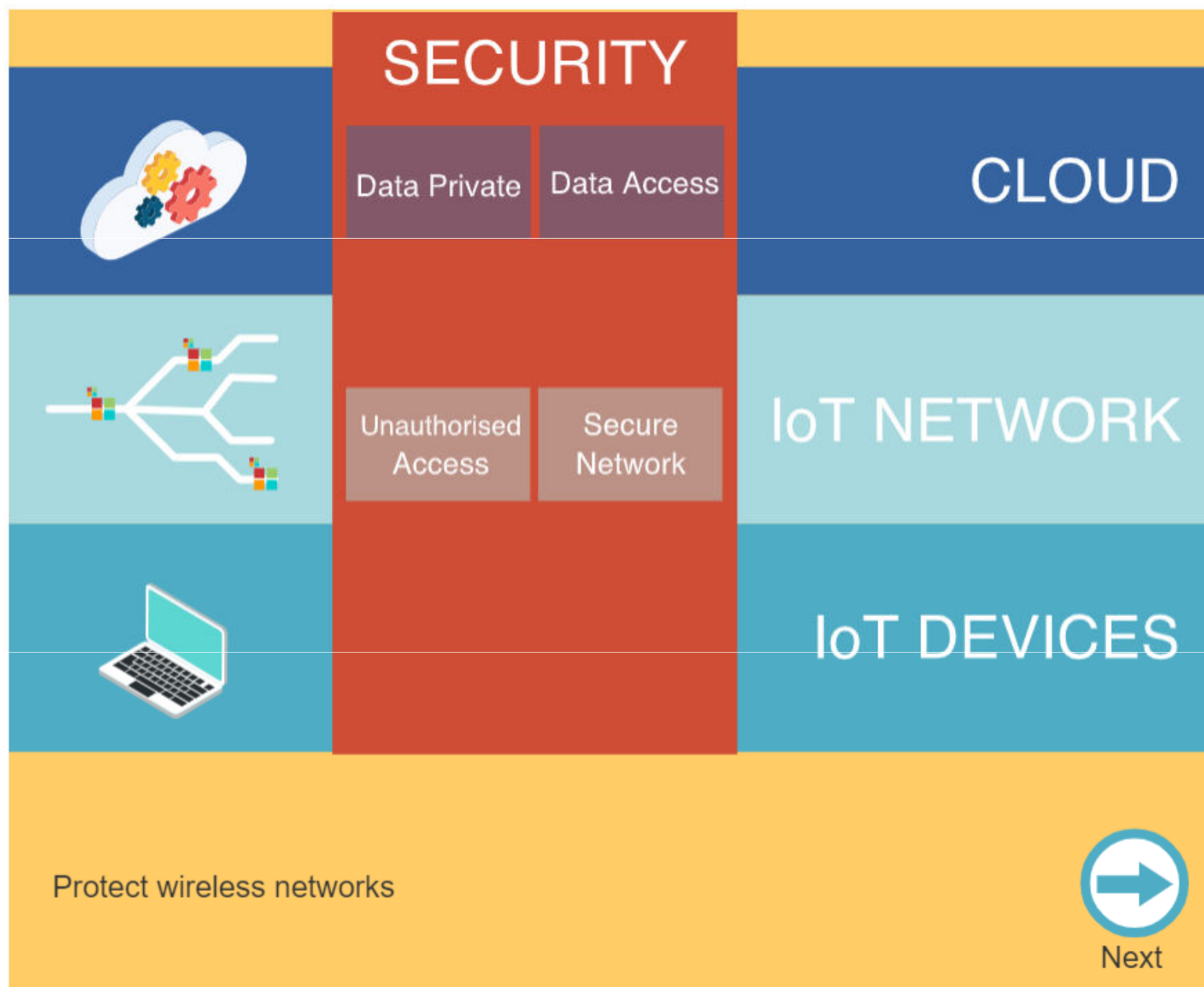
Security Issues Related to IoT (cont.)



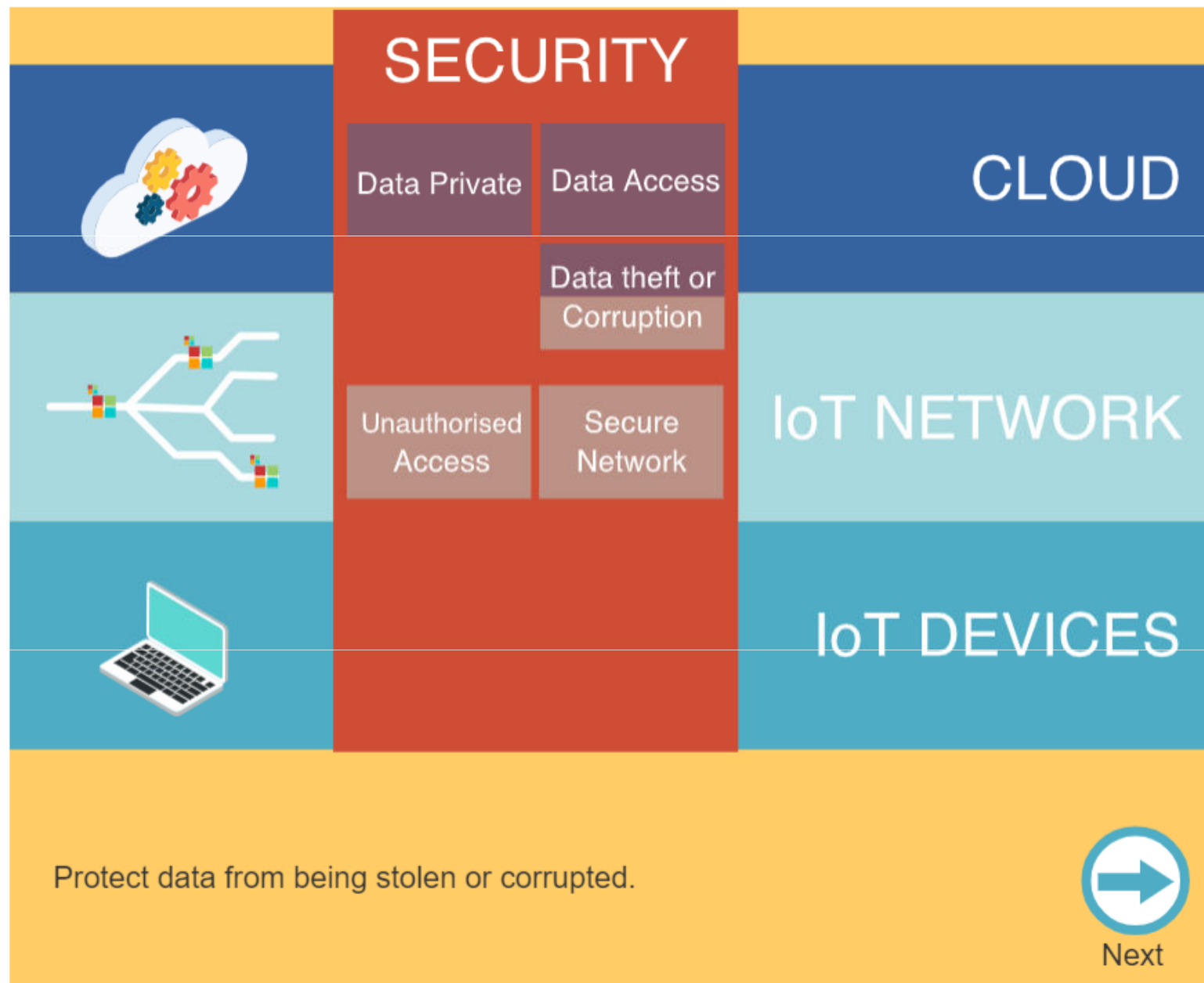
Security Issues Related to IoT (cont.)



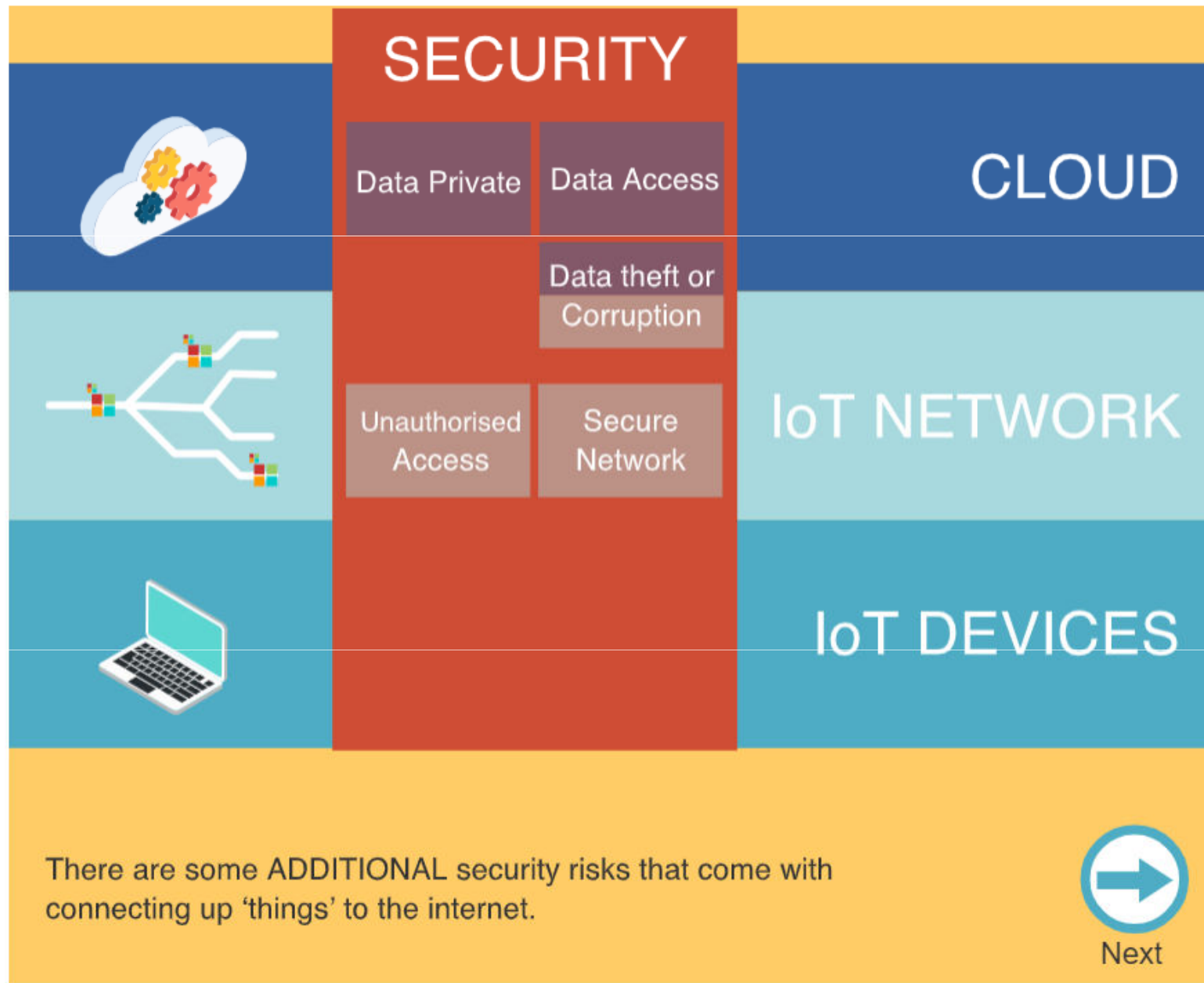
Security Issues Related to IoT (cont.)



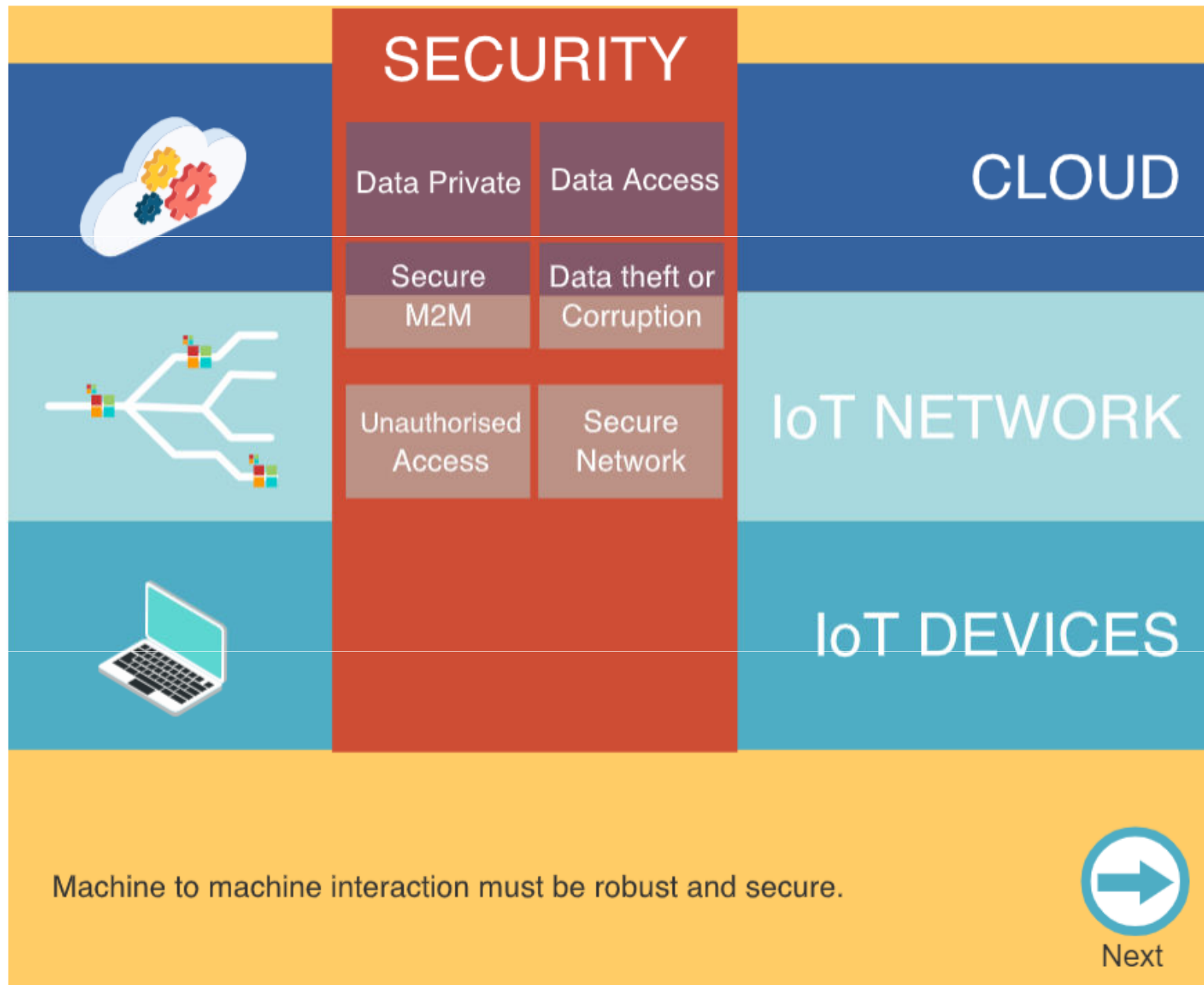
Security Issues Related to IoT (cont.)



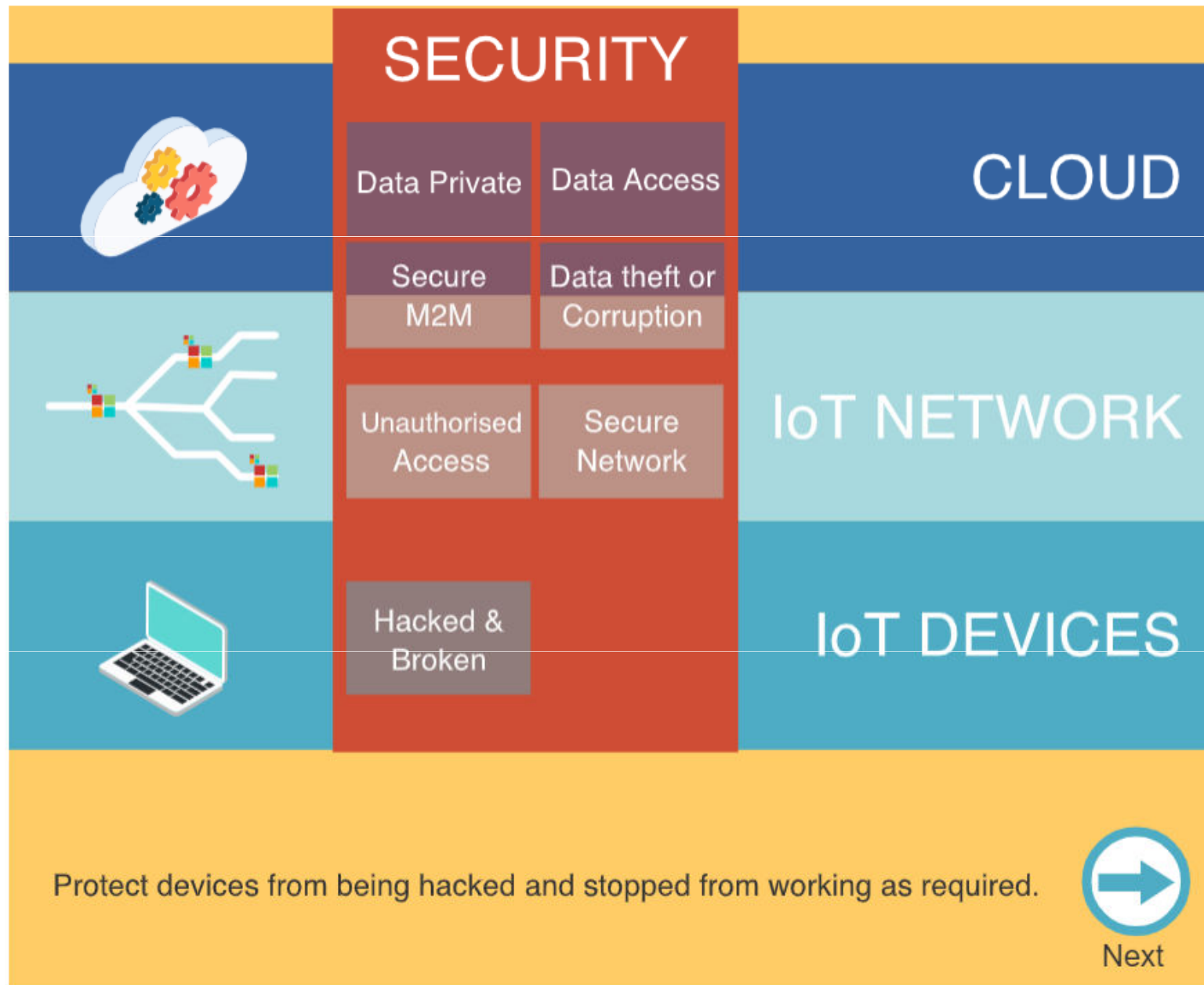
Security Issues Related to IoT (cont.)



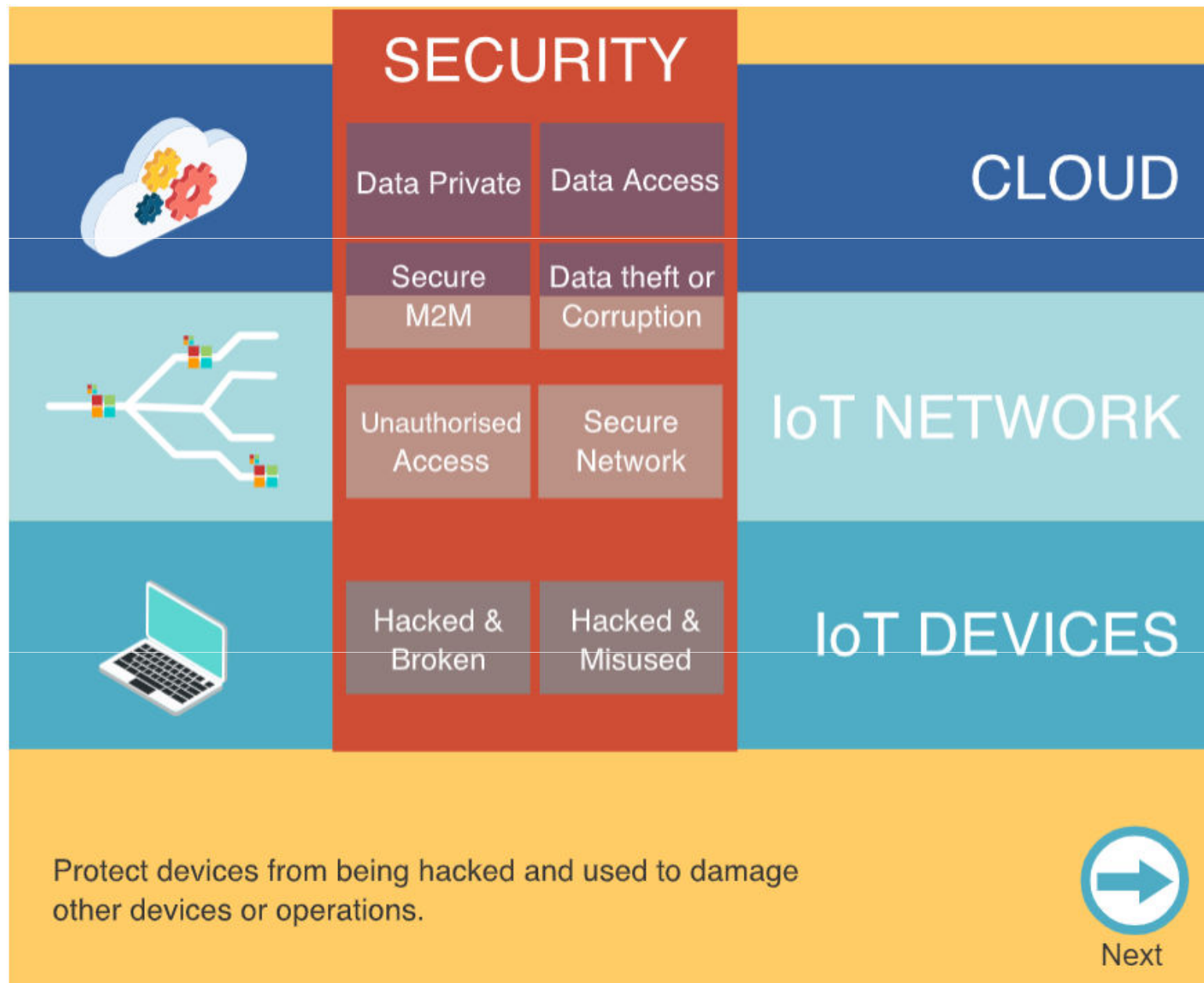
Security Issues Related to IoT (cont.)



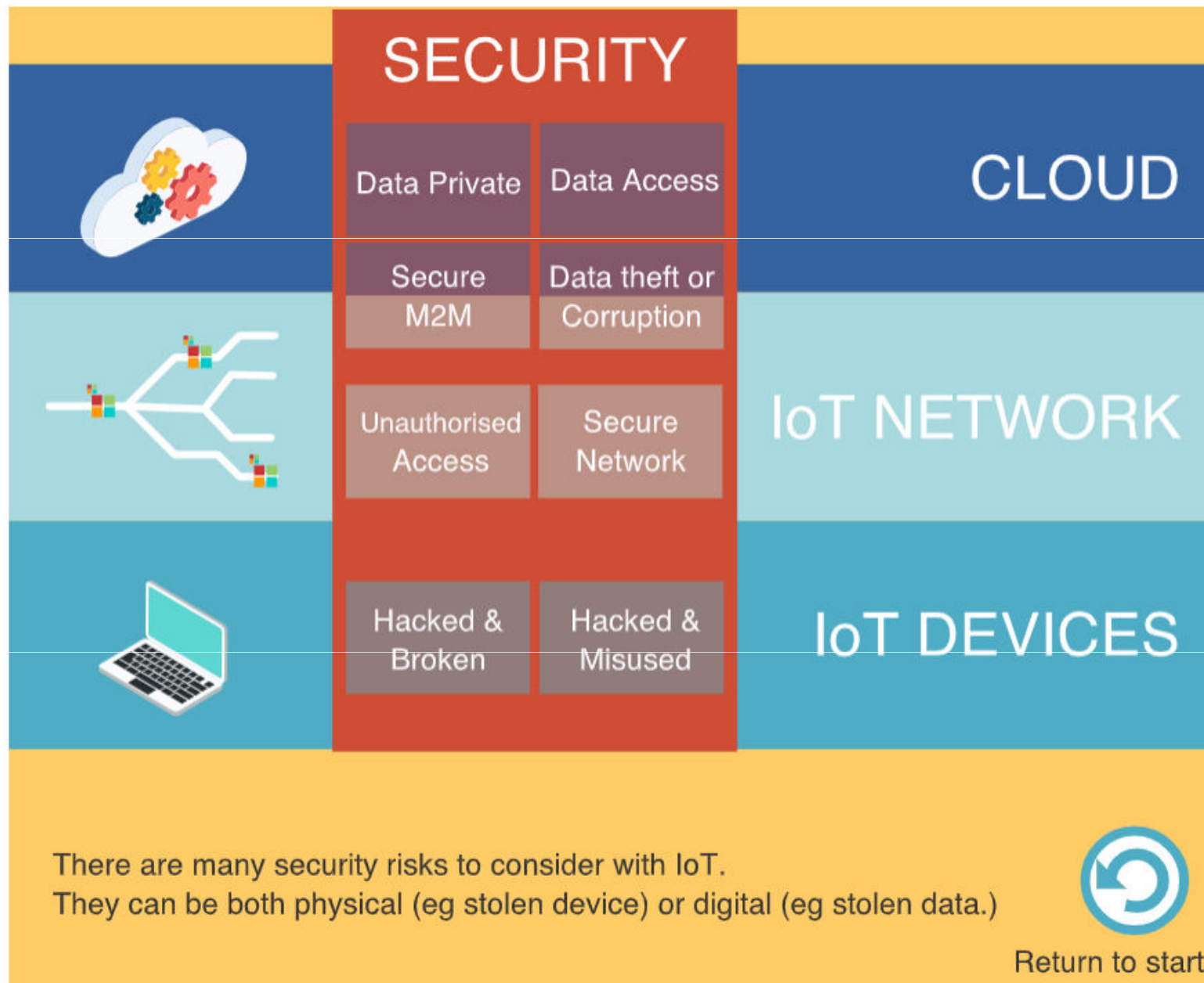
Security Issues Related to IoT (cont.)



Security Issues Related to IoT (cont.)



Security Issues Related to IoT (cont.)



Privacy and Ethics



- Data may be collected from people (with or without their knowledge) through IoT includes: personal information; locations and movements; habits; physical conditions.
- Personal data valuable to sales and marketing, service planning, health intervention, credit decisions, insurance decisions, employment decisions, fraud and theft.
- Good product development practice involves developers: conducting a privacy and security risk assessment, building security into the product from the outset, testing the security measures before launching, using a service provider capable of providing security, and monitoring a product through its life cycle.

Privacy and Ethics (cont.)

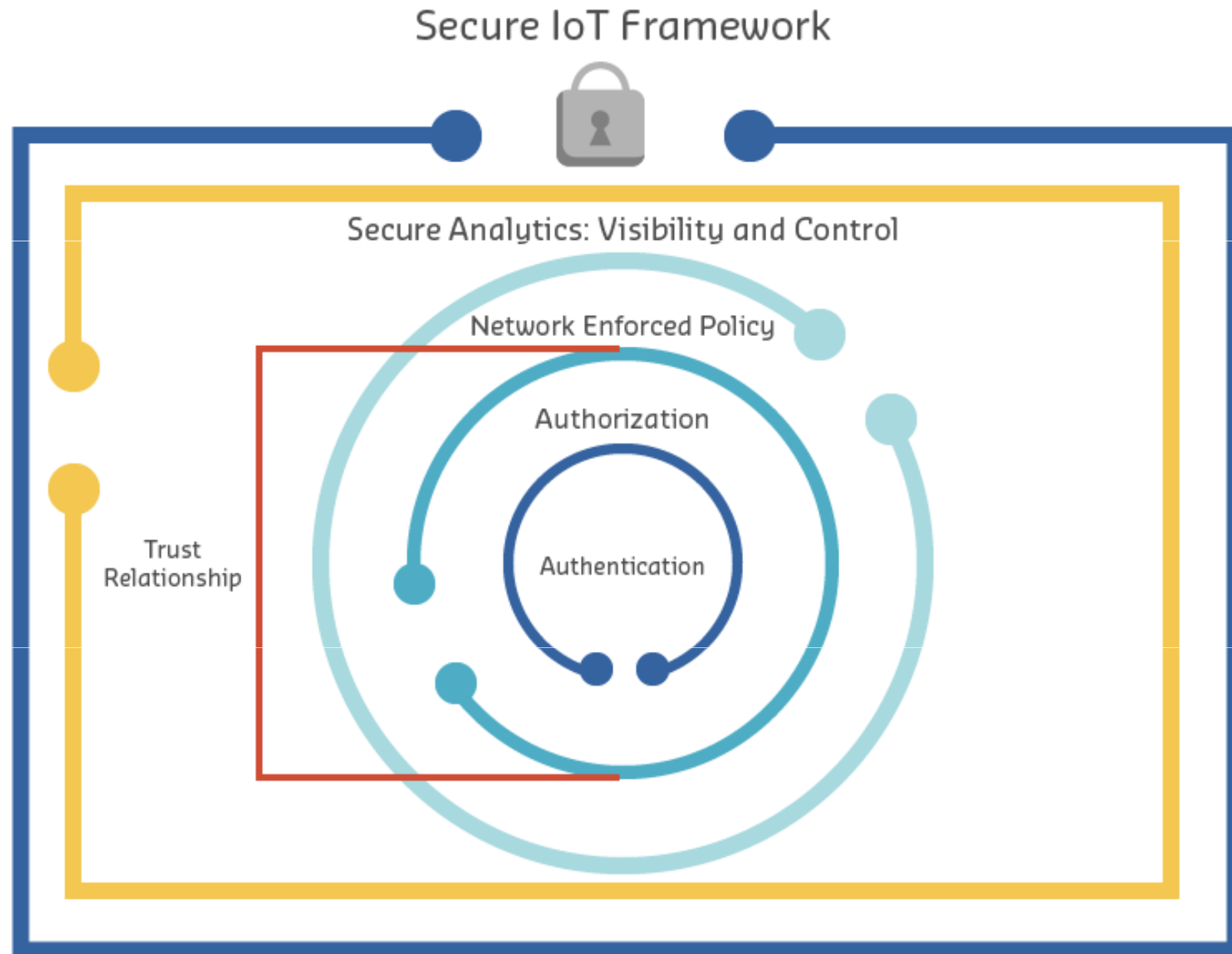


- Due to additional privacy and security risks, other recommendations around IoT development are to minimize the data collected and retained, and the length of time data is retained, to consider who should have access to data (at the appropriate level in an organization), and to educate employees about good security practices.
- The Federal Trade Commission (FTC) report refers to Fair Information Practice Principles, or FIPPs. 4 FIPPs were focused on, i.e., notice (consumer being given notice of practice), choice (consumer having control over how data is used), data minimization, security (consumers' held data being accurate and secure).

Cyber Security Methods

- IoT devices can connect a person's activity to their identity, which presents a challenge to privacy.
- A device does need to be able to check ownership and identity, but it also needs to de-couple (separate) itself from the owner. This is called **shadowing**. The device uses a virtual identity to act on behalf of the owner (whom it knows about, but does not reveal the identity of).
- The following diagram from the Cisco Networking Academy shows an example of a Secure IoT Framework.

Cyber Security Methods (cont.)



Cyber Security Methods (cont.)

It outlines the following components:

- **Authentication** – IoT devices connecting to the network create a trust relationship, based on validated identity through mechanisms such as: passwords, tokens, biometrics, RFID, X.509 digital certificate, shared secret, or endpoint MAC address.
- **Authorization** – a trust relationship is established based on authentication and authorization of a device that determines what information can be accessed and shared.
- **Network Enforced Policy** – controls all elements that route and transport endpoint traffic securely over the network through established security protocols.
- **Secure Analytics: Visibility and Control** – provides reconnaissance, threat detection, and threat mitigation for all elements that aggregate and correlate information.

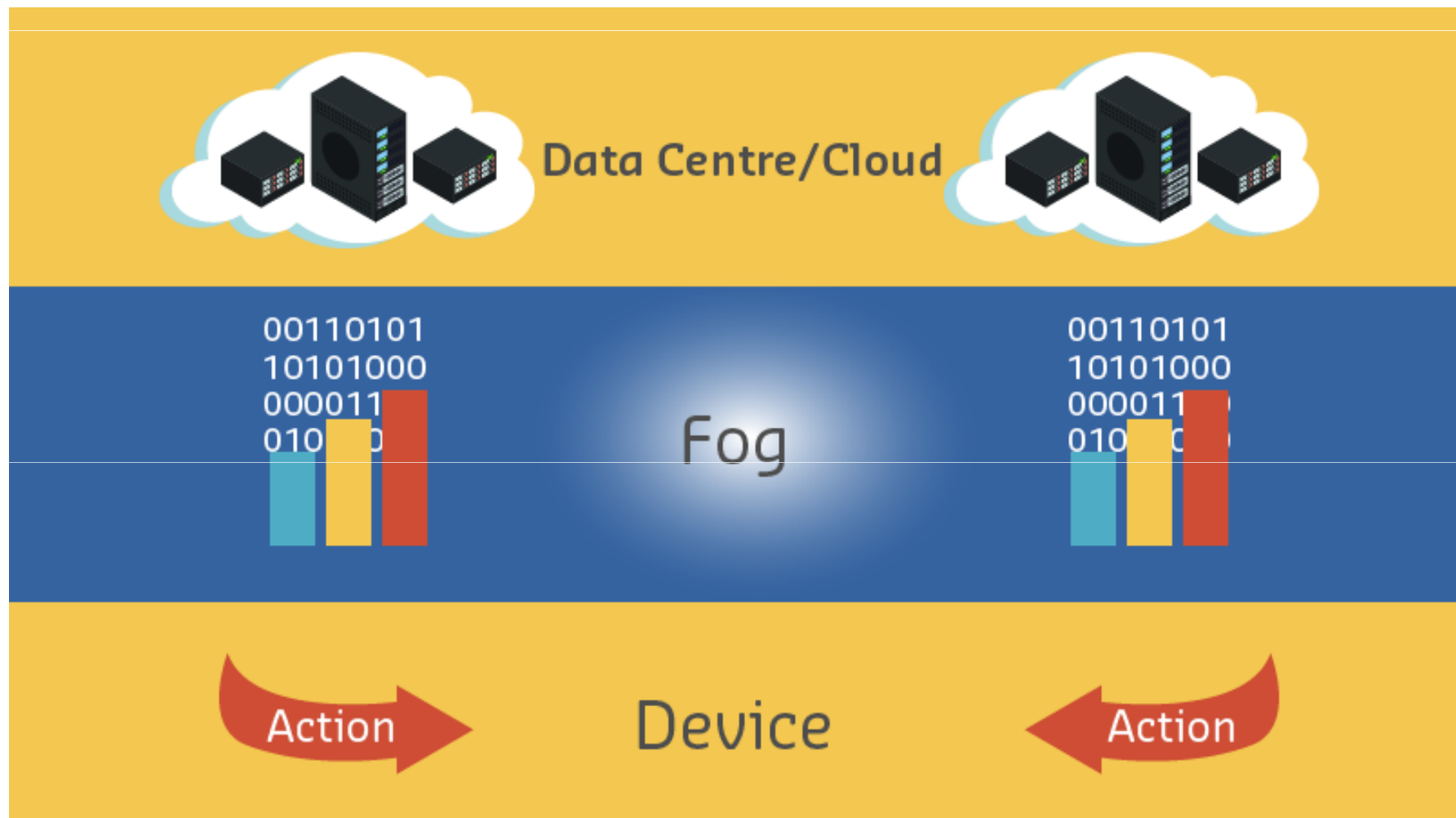
Off The Shelf IoT

- If you're using an 'off the shelf' IoT product, don't forget the following additional security measures:
 - Disable default passwords
 - Disable UPnP (Universal Plug and Play - which allows the device to automatically make itself available to networks)
 - Disable remote management
 - Keep software (firmware) up to date
 - Use encryption and/or certificates where possible
 - Physically keep device secure

off the shelf: not designed or made to order but taken from existing stock or supplies.

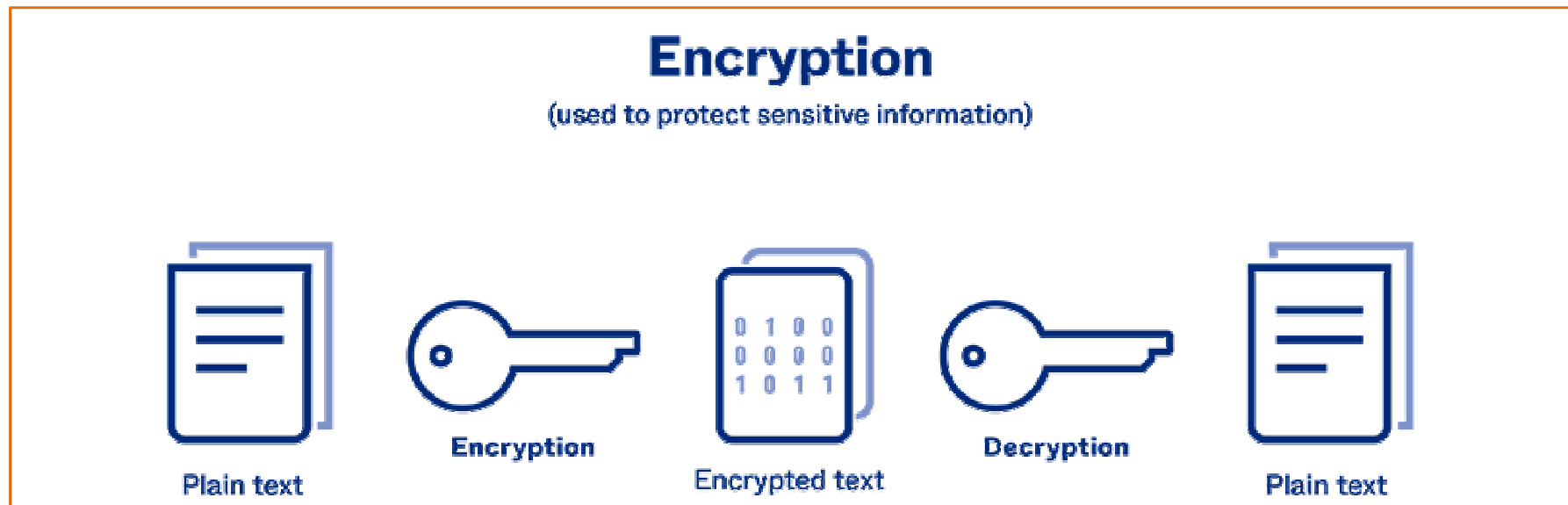
Fog Computing

- Another way to increase the security of IoT devices, is to use 'the fog'. The fog extends the reach of 'the cloud', so it is closer to devices that create and act on IoT data.





Encryption

- Encryption is an important form of computer security. Encryption simply involves encoding a message or information.



- Encryption simply involves encoding a message or information. You probably engaged in some simple encryption when writing secret notes as a child, replacing letters with other letters, numbers or characters, or writing in invisible ink and needing a UV light to expose the message. Computer encryption uses the same basic principles.



Identifying IoT Security Risks

MEDICAL SCENARIO	Risks	Impact of risk	Likelihood of risk event	How to avoid/lessen the risk
<div>Wearable heart monitor</div> 	Data theft	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Encryption</div> <div>Authentication, password protect</div>
<div>Medical data in the Cloud</div> 	Data theft, privacy compromised	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Remove identification from data</div> <div>Control access to private data</div>

- Wearable heart monitor: Encryption, Authentication, password protection.
- Medical data in the Cloud: Remove identification from data, Control access to private data.



Note: Although you will need to line up solutions with the risks, there is no 'correct' answer for the 'Impact of risk' or 'Likelihood of risk event' categories – this is an exercise in practicing risk analysis, so your answer should reflect what you think.

Identifying IoT Security Risks (cont.)

AGRICULTURAL SCENARIO	Risks	Impact of risk	Likelihood of risk event	How to avoid/lessen the risk
Microcontroller 	Malicious control of device	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Use established security protocols</div> <div>Hide, physically lock away or protect</div>
Solenoid valve water release 	Physically damaged	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Select...</div> <div>Select...</div>

- **Microcontroller:** Encryption, Authentication, password protection. Also relevant are: Use established security protocols, Hide or physically lock away devices, Keep firmware updated.
- **Solenoid valve water release:** Threat detection, firewall, Physically lock away or protect device.

Identifying IoT Security Risks (cont.)

INDUSTRIAL SCENARIO	Risks	Impact of risk	Likelihood of risk event	How to avoid/lessen the risk
Data in network 	Data corruption	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Use Fog/edge computing ▾</div> <div>Authentication, password protect ▾</div>
Manager with computer and tool kit 	Data corruption	Impact level? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	Risk likelihood? <input type="checkbox"/> High <input type="checkbox"/> Medium <input type="checkbox"/> Low	<div>Hide, physically lock away or protect ▴</div> <div>Authentication, password protect ▾</div>

- Data in network: Use Fog/edge computing, Authentication, password protect.
- Manager with computer and tool kit: Hide, physically lock away or protect device or computer, Authentication, password protection.



THANK YOU ALL FOR LISTENING





QUESTIONS AND ANSWERS