Security Management in an IoT Driven World.

Sean Gulliford – Principal Consultant

IoT Security Foundation

Gemserv

Internet of Things

“The Times They Are a Changin.”

Bob Dylan

Real world challenges

Greater reliance on the digital economy

“Without the investment needed to cope with developments such as automation and the adoption of digital services, the commission warns, the UK is likely to face another decade of stagnant wages, rising household debts and deteriorating infrastructure”

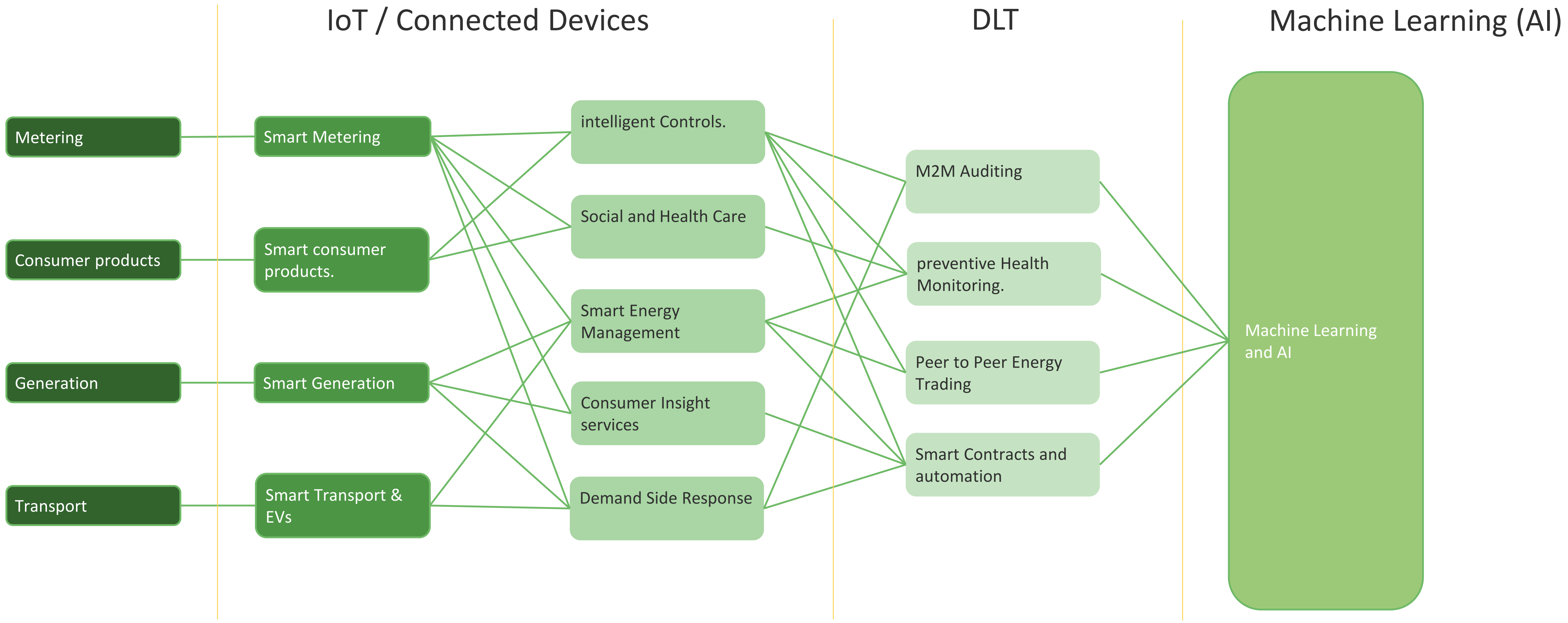
Intergovernmental Panel on Climate Change (IPCC)

We need to rapidly move away from traditional fuels to cleaner renewable forms of Energy.

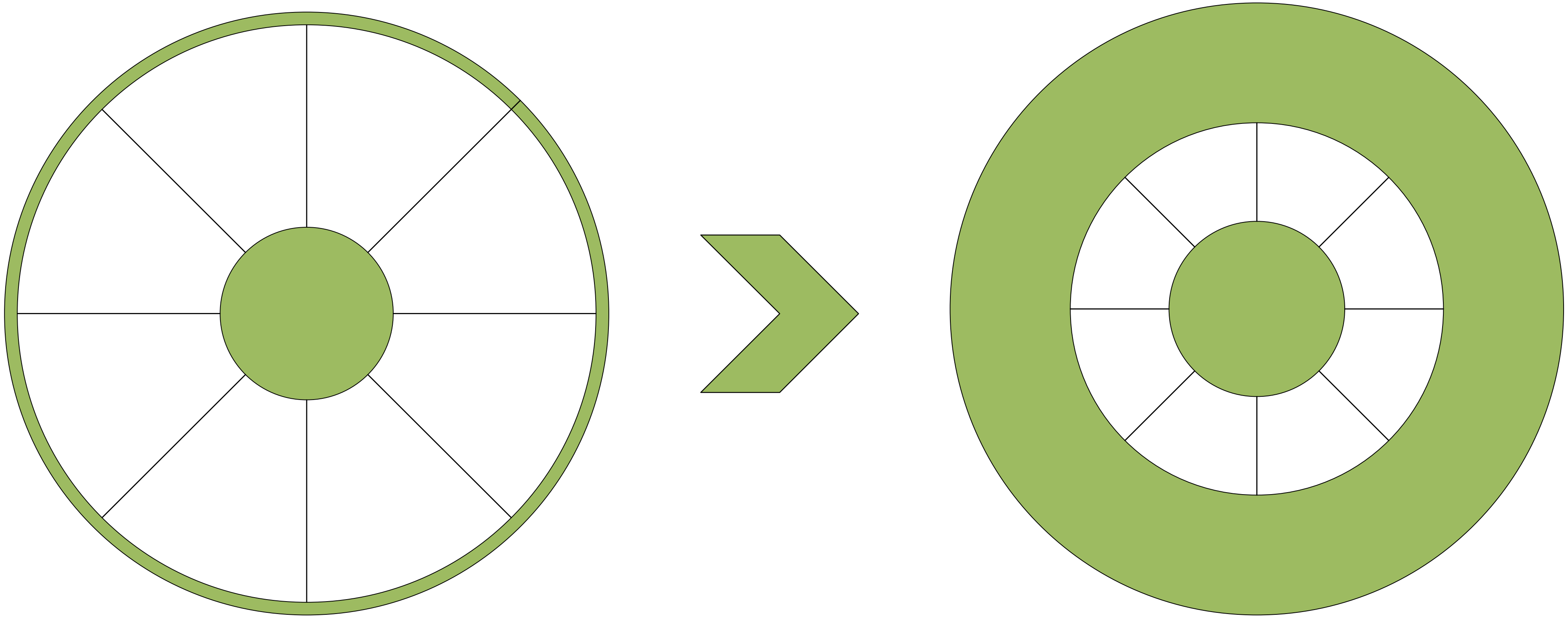
Market Drivers (Energy)

- Electric Vehicles and the decline of diesel
- Increased use of renewable energy
- Battery Storage
- Demand Side Response
- Peer to peer energy trading

Blurring Market Verticals



Cloud to Fog



Regulatory Drivers

"The controller shall..implement **appropriate technical and organisational measures**..in an effective way.. in order to meet the requirements of this Regulation and protect the rights of data subjects"

https://www.eugdpr.org/the-regulation.html

"One of the key objectives of the NIS Directive is to ensure that Operators of Essential Services (OES) take **appropriate and proportionate technical and organisational measures** to manage the risks to the security of network and information systems which support the delivery of essential services"

https://www.ncsc.gov.uk/guidance/introduction-cyber-assessment-framework

Best Practice Initiatives (Future Regulations)

Secure by Design

“Manufacturers of 'smart' devices will be expected to build-in tough new security measures that last the lifetime of the product”

“Poorly secured devices threaten individuals’ online security, privacy, safety, and could be exploited as part of large-scale cyber attacks”

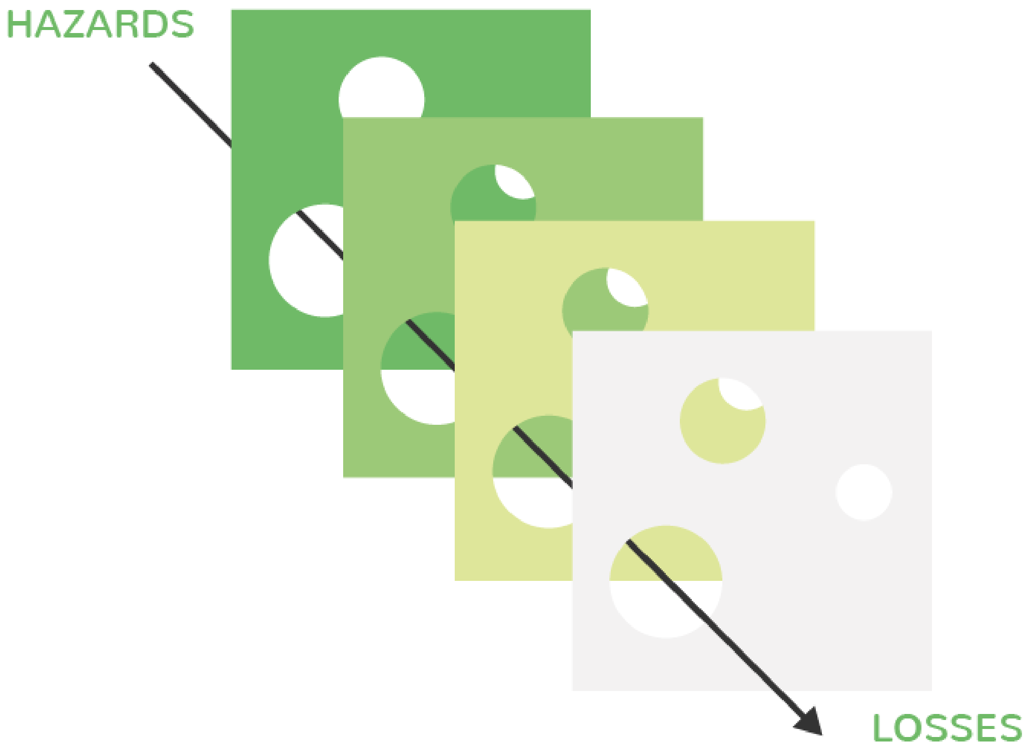
https://www.gov.uk/government/news/new-measures-to-boost-cyber-security-in-millions-of-internet-connected-devices

The first step

Don’t Reinvent the Wheel

A Layered approach

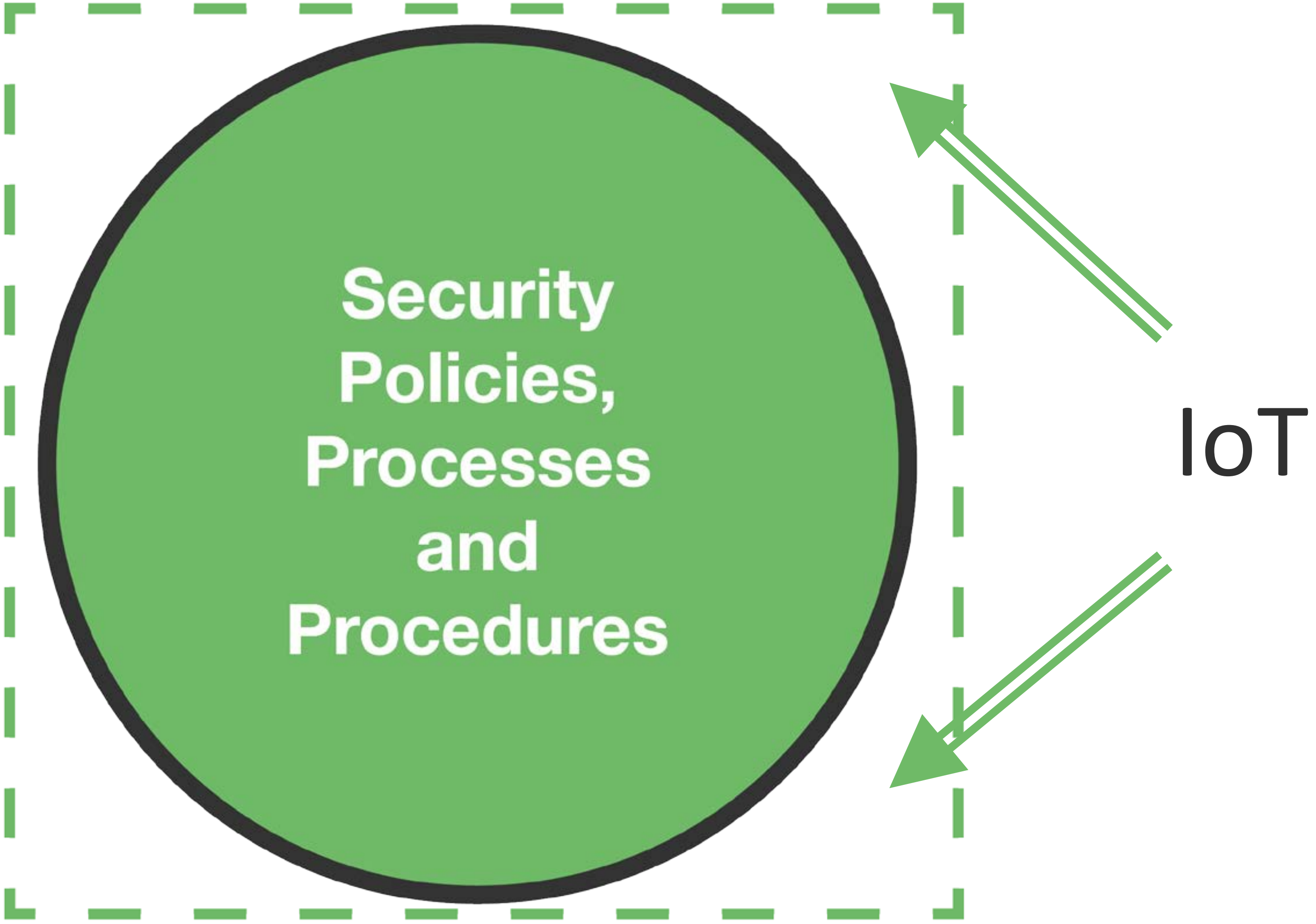
- Security requires socio-technical response:
  - People, Processes and Technology
- a multi layer defensive approach driven from the top



Understand

Security Policies, Processes and Procedures

Adapt

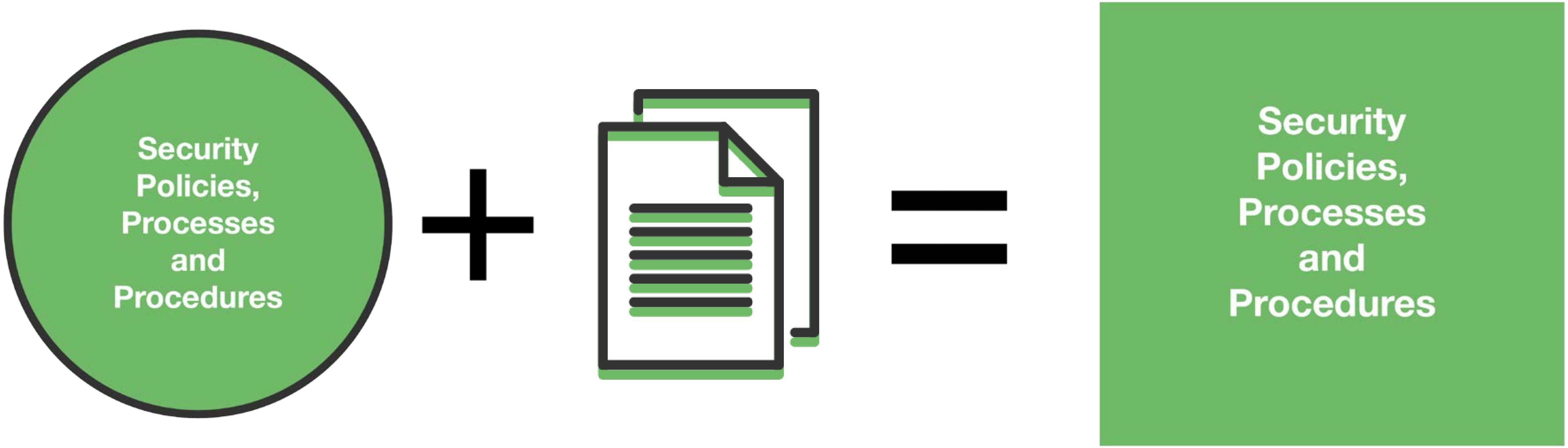


Security Policies, Processes and Procedures

IoT

Filling the Gaps

- Review Existing Polices, processes and procedures in light of IoT.
- Use the IoTSF compliance framework.


Security Policies, Processes and Procedures
+
=
Security Policies, Processes and Procedures

Understand what is Appropriate ?

Use a risk based approach:

- What's on the network?
- What does it do?
- what data does it process?
- What is its security characteristic?
- Who is responsible for maintaining it?
- Are there controls in place to ensure and maintain security?

ISO27001 Scoping

- 4.1 – Understand the Organisation and its context:
  - Does the Organisation utilise IoT?
- 4.3 – Determine the Scope of the ISMS:
  - Is the IoT included in the scope and high level asset discovery?
- 5.2 - Information Security Policy:
  - Are IoT Devices included within the information Security Policy documentation?
- 5.3 – Roles and responsibilities:
  - Which business units are responsible for IoT?

6.1.2 – Risk Assessment:

  - Are IoT Devices included in the risk assessment?

Asset Management is key

- You can accurately access the risks.
- You understand the security characteristics.
- You can modify existing process.
- You understand the gaps.
- You can ensure that IoT is in Scope.

Key Areas

Procurement

- Identify IoT Devices.
- Is there a business case?
- Understand their Security characteristics?
- Understand any regulatory obligations:
  - What Data does is process ?

Installation and Configuration

- Who is responsible for installing and commissioning.
- Co-ordination between business units:
  - Facilities management, IT.
- Where does it sit in the network?
  - Will additional controls be required?
- What Data does is process?

In-life Maintenance

- Who is responsible for in-life maintenance:
  - Internal.
  - Supplier.
- What are their obligations?
- How long will the device be supported?
- Are there communication channels in place:
  - Internal and external.
  - Vulnerability Reporting.
- Training.

In summary - What now?

- Are there IoT devices on the network?
- What data do they handle?
- What do they do ?
- What risk do they pose to network?
- Are there Policy's, processes and procedures in place to address IoT Devices
    - Procurement, maintenance, installation, commissioning, ongoing support etc.

Moving Forward

- Ensure that IoT devices and systems have appropriate security characteristics before installation.
- Understand who is responsible for maintaining them and for how long.
- Include IoT devices into the scope of ongoing security assessments.
- Apply a “not if, but when” approach.

Privacy and Security

“The companies that do the best job on managing a user’s privacy will be the companies that ultimately are the most successful"

Fred Wilson

“Privacy and security are two sides of the same coin. We cannot have one without the other”

Richard A Clark

In conclusion

Further Information

https://www.gemserv.com/we-need-to-talk-about-this-iot-thing/

Thank you for listening.

Any Questions?

Sean.Gulliford@Gemserv.com