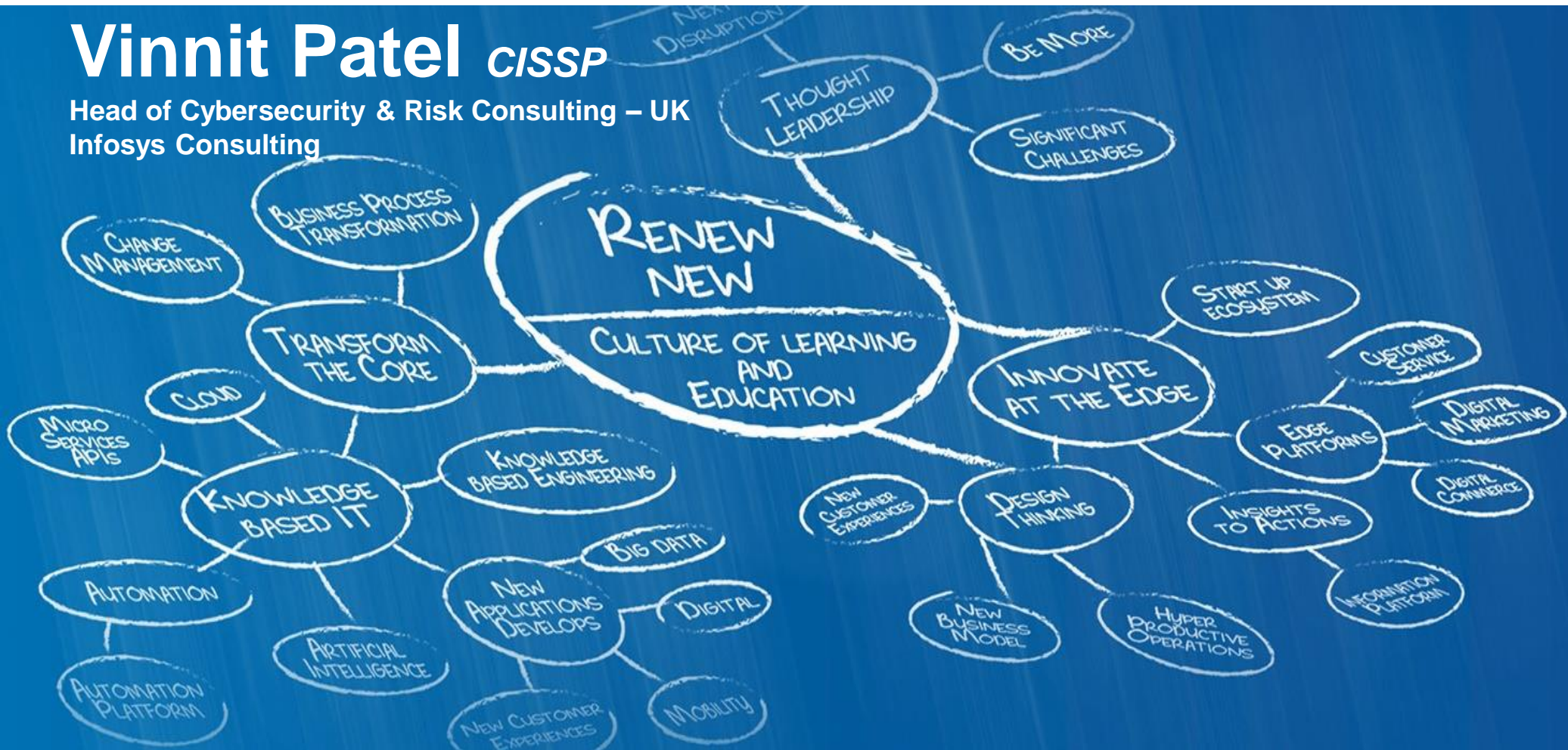


# Data Security in Oil & Gas

Key Cybersecurity Trends with a focus on data security

**Vinnit Patel** *CISSP*

Head of Cybersecurity & Risk Consulting – UK  
Infosys Consulting



# Quick Bio!

## Vinnit Patel *CISSP*

+19 Years in IT/Information Security, Risk & Compliance

### Specialities:

- Cybersecurity Strategy
- Identity & Access Management
- Infrastructure Security
- Data Protection
- Clarifying new data regulations
- Security Operations
- Governance, Risk & Compliance

Dayjob = Head of Cybersecurity & Risk Consulting

Sidejob = Senior Principal Consultant for projects at BP, Centrica, HSBC among others.



# What We'll Cover

**1** *Cyber attack Trends*

**2** *Threat Actors*

**3** *Motivation of Threat Actors*

**4** *Practical Steps to help Protect your Data*

**5** *GDPR – So What?*

**6** *In Summary*



**1** *Cyber attack Trends*

**2** *Threat Actors*

**3** *Motivation of Threat Actors*

**4** *Practical Steps to help Protect your Data*

**5** *GDPR – So What?*

**6** *In Summary*

# Cyber attacks – it won't happen to us!

## “NHS crippled in global cyber attack – 2017”



- Operations were cancelled and ambulances diverted at over 50 hospital trusts
- NHS IT systems were unavailable for several days

## “Renault shut down factories after cyber attack – 2017”



RENAULT

- Activity was suspended at several sites a cyber attack forced them to take proactive measures
- Factories were closed for several days, leading to an estimated \$140 million in lost production

## “Virus targets energy sector infrastructure – 2015”



- Saudi Aramco, Saudi Arabia's national oil company, 35,000 computers wiped in hours as a result of a computer virus
- It took the company a week to restore their IT services to normal

## “Cyber Attack Disrupting Website - 2012”



- Wells Fargo online banking website was hit by a cyber attack
- The attacks were to keep customers from accessing their accounts, causing loss of business

## “Yahoo biggest data breach in history – 2013 & 2014”



- Names, passwords and email addresses were stolen during an attack
- The sale of Yahoo's internet business to Verizon was cut by \$350 million as a result of the data breaches

## “Former employees suing Sony over Hack - 2014”



- The hack led directly to the departure of Sony Pictures chairman Amy Pascal
- Sony paid over \$5.5 million to end the class action lawsuit
- Analysts estimate the total cost of the data breach to be \$1.25 billion

## “TalkTalk...record £400k fine & £60M in losses - 2015”



- Personal data, including sensitive financial data, of over 150,000 people was stolen
- Lost 101,00 customers and suffered costs of £60m as a result of the attack

## “eBay faces investigations over data breach - 2014”



- Personal data of over 145 million customers was stolen
- Ebay faces a fine of up to £500,000
- Lowered annual sales target by \$200 million as a direct result

# Hacker Group Anonymous Launches #OpPetrol to Target Global Oil Industry



Anonymous targets global oil trade in new cyber attack campaign



The oil and gas industry has found itself in the crosshairs of hacker activist group Anonymous, which recently announced plans to launch cyber attacks on countries involved in the global oil trade.



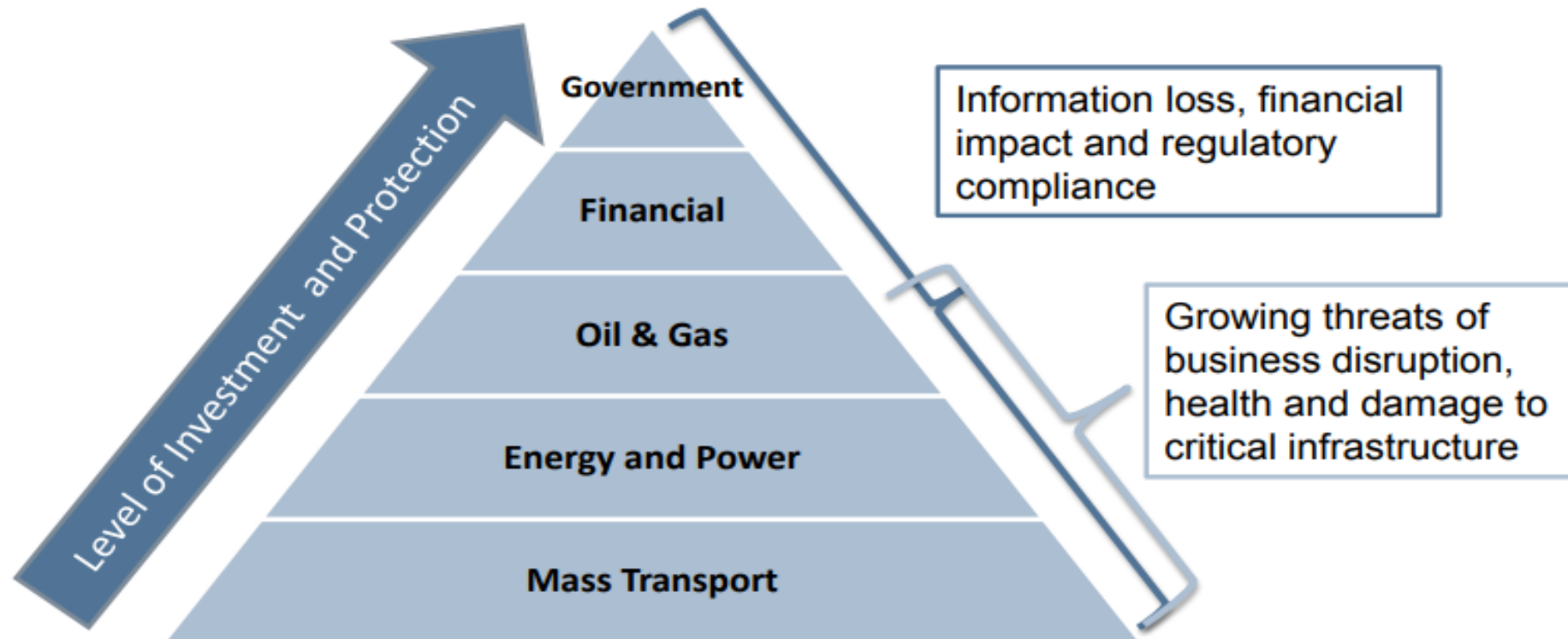
# Should I Worry??





# Attacks aimed at Critical National Infrastructure (CNI)

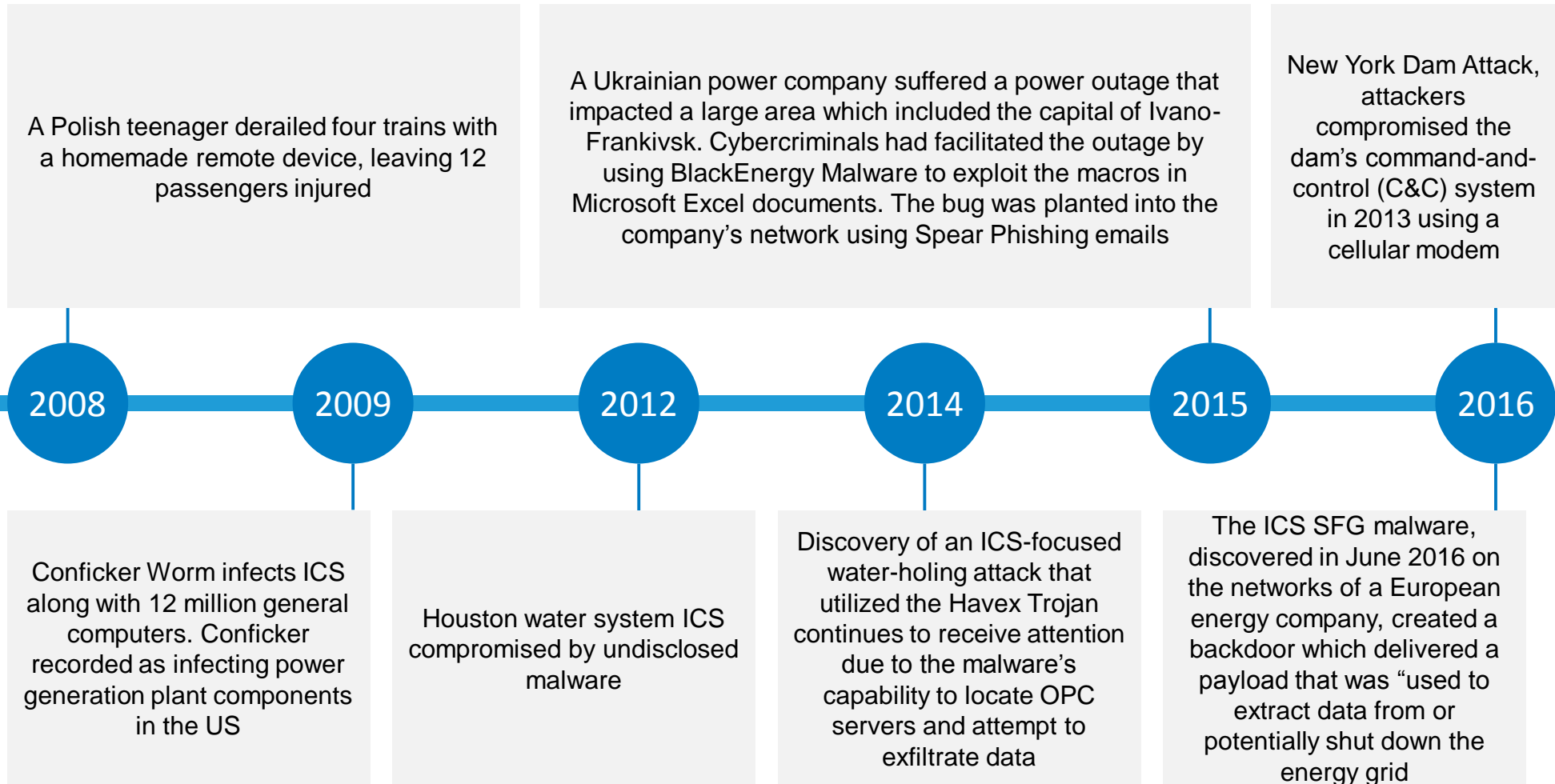
- Financial services has been quicker to adopt more advanced security solutions than other CNI sectors
- Greatest attacks still aimed at Oil & Gas / Energy and Utilities sectors



***An average of 46 percent of all cyber attacks in the Operation Technology environment go undetected!!***  
*Source: Ponemon Institute – sponsored by Siemens*



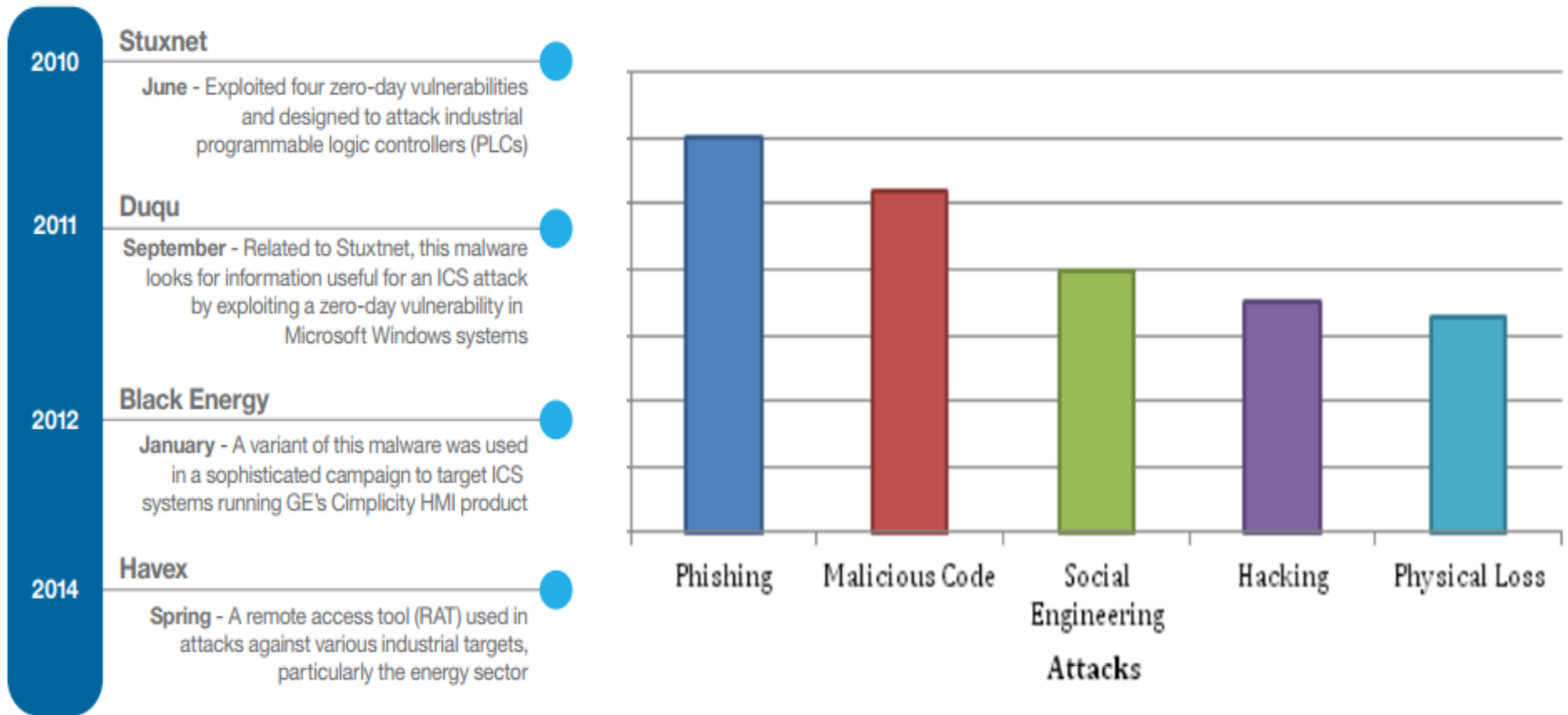
# Notable Recent Industrial Control Systems (ICS) Attacks



**Attacks Targeting Industrial Control Systems (ICS) Up 110 Percent**

source: SecurityIntelligence

# Top 5 Successful Attacks across all Industries



**Oil and Gas industries have seen an increase in successful cyber attacks over the past 12 months**

Source: Ponemon Institute – sponsored by Siemens

**1** *Cyber attacks Trends*

**2** *Threat Actors*

**3** *Motivation of Threat Actors*

**4** *Practical Steps to help Protect your Data*

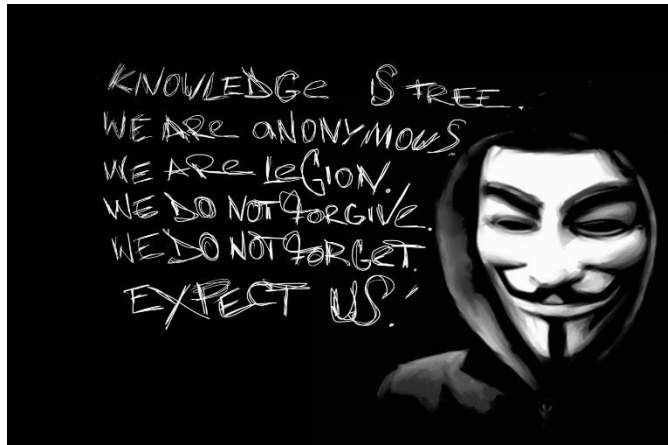
**5** *GDPR – So What?*

**6** *In Summary*



# Understanding the 4 Main Threat Actor Types

## Hacktivists



## State-Sponsored Attackers



## The Insider Threat



## Organized Cyber Criminals



1 *Cyber attacks Trends*

2 *Threat Actors*

3 ***Motivation of Threat Actors***

4 *Practical Steps to help Protect your Data*

5 *GDPR – So What?*

6 *In Summary*

# Motivations of Threat Actors

## Hacktivists

Not motivated by money. Instead, they have a burning rage inside them that for whatever reason has been directed at *you*.

## State-Sponsored Attackers

Less common than cyber crime and hacktivism, but are a real and concerning threat. They want your data, If your organization operates in a particularly sensitive market you're at a greater risk of gaining the attentions of a state-sponsored hacking group.

## The Insider Threat

May be employees falling victim to social engineering or phishing attacks, disgruntled employees seeking revenge. Steal data for resale on the dark web but most commonly are User accounts which have been compromised by an external attacker.

Hard to distinguish these actions from all the legitimate activity that occurs every day on your network. Insider threats are dangerous, and often hard to spot.

## Organized Cyber Criminals

Has overtaken the drug trade to become the most profitable illegal industry, it's estimated that victims in the U.S. paid over \$24 million in 2015 to groups using ransomware trojans, and that's just one attack vector.

They are well equipped, well funded, and they have the tools and knowledge they need to get the job done.



1 *Cyber attacks Trends*

2 *Threat Actors*

3 *Motivation of Threat Actors*

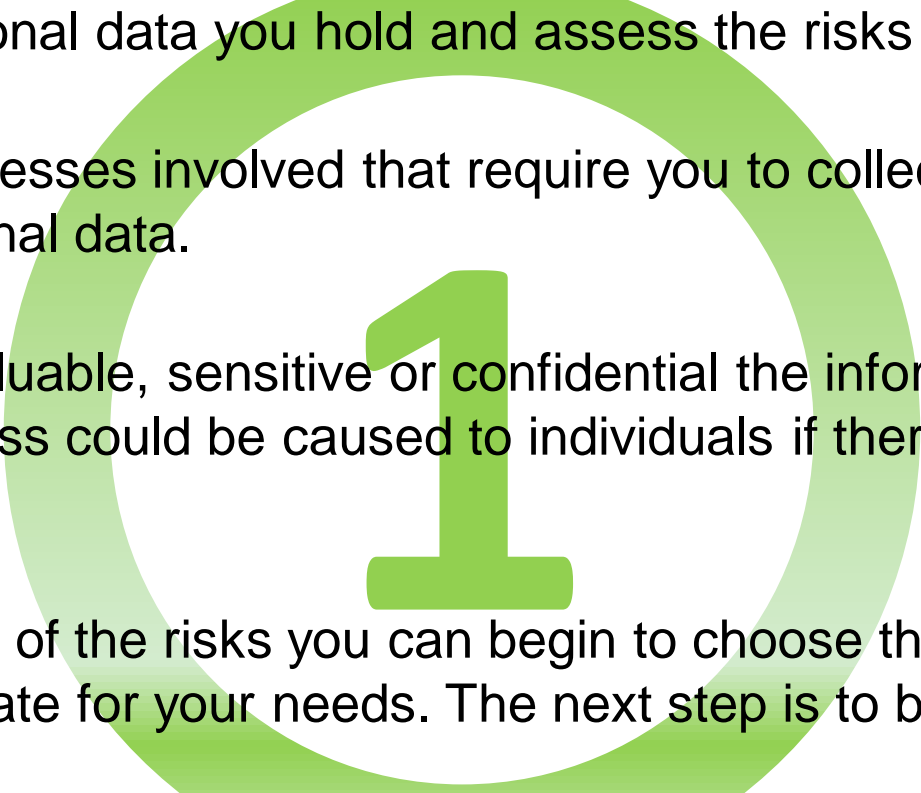
4 ***Practical Steps to help Protect your Data***

5 *GDPR – So What?*

6 *In Summary*

# Practical steps to help protect your data

## Assess the threats and risks to your business

- 
- Review the personal data you hold and assess the risks to that data.
  - Consider all processes involved that require you to collect, store, use and dispose of personal data.
  - Consider how valuable, sensitive or confidential the information is and what damage or distress could be caused to individuals if there was a security breach.
  - With a clear view of the risks you can begin to choose the security measures that are appropriate for your needs. The next step is to begin putting them in place.

# Practical steps to help protect your data

## Define and establish and effective Information Security Policy

- Policy Statements are one thing, how do these translate into implementation of effective controls?
- Ensure your Policy is underpinned by Standards which explain how to implement and operate the required controls
- Ensure you Standards are underpinned by Processes with accountable process owners, responsible control owners and control executors



2



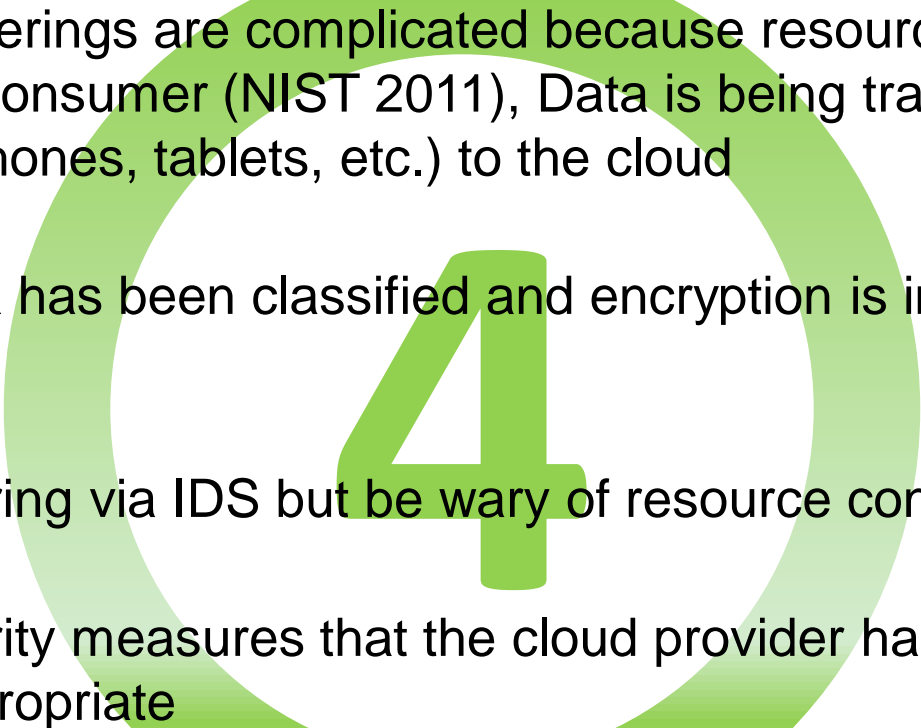
# Practical steps to help protect your data

## Secure your data on the move and in the office

- Physical security is important! Many data breaches arise from the theft or loss of a device (e.g. laptop, mobile phone or USB drive)
- Consider full disk encryption, file encryption, power on passwords, MDM
- Plan and implement: Firewalls/Internet Gateways, Secure Configuration, Access Controls, Malware Protection, Patch Management & Software Updates, Encryption (HDE/RME), FIM, Security Testing, Logging & Monitoring, Incident Response, Governance,...etc.

# Practical steps to help protect your data

## Secure your data in the cloud

- 
- Cloud service offerings are complicated because resources are shared and unknown to the consumer (NIST 2011), Data is being transferred from IoT (laptops, smartphones, tablets, etc.) to the cloud
  - Ensure your data has been classified and encryption is in place for sensitive data
  - Consider Monitoring via IDS but be wary of resource consumption!
  - Assess the security measures that the cloud provider has in place to ensure that they are appropriate

# Practical steps to help protect your data

## Back up your data

- In the event of a disaster such as fire, flood or theft you need to be able to get back up and running as quickly as possible. Loss of data is also a breach of the DPA and soon to be GDPR which takes effect May 2018
- Malware can also disrupt the availability of access to your data. Known as 'ransomware' this type of malware can encrypt all your data and only provide you with the means to decrypt the data after payment of a ransom
- Back-ups should not be stored in a way that makes them permanently visible to the rest of the network. If they are then they can be encrypted by malware or the files accidentally deleted



# Practical steps to help protect your data

## Make sure your IT contractor is doing what they should be

- Be satisfied that they are treating your data with at least the same level of security as you would
- Ask for a security audit of the systems containing your data. This may help to identify vulnerabilities which need to be addressed
- Review copies of the security assessments of your IT provider
- Visit the premises of your IT provider to make sure they are as you would expect
- Check the contracts with your IT providers ensure they will comply with certain obligations
- Don't overlook asset disposal – if you use a contractor to erase data and dispose of or recycle your IT equipment, make sure they do it adequately. There is a risk that sensitive or personal data is extracted from your old IT equipment when it is resold

# Practical steps to help protect your data

## Keep an eye out for problems

- Many people only find out they have been attacked when it is too late even though the warning signs were there.
- Check your security software messages, access control logs and other reporting systems you have in place on a regular basis (via the SOC)
- Act on any alerts that are issued by these monitoring services (e.g. SIEM)
- Run regular vulnerability scans and penetration tests to scan your systems for known vulnerabilities – make sure you address any vulnerabilities identified.

# Practical steps to help protect your data

## Know what you should be doing

- A good policy will enable you to make sure you address the risks in a consistent manner. Well written policies should integrate well with business processes.
- Document the controls you have in place and identify where you need to make improvements.
- Consider the risks for each type of data you hold and how you would manage a data breach. This way you can reduce the impact if the worst was to happen.

# Practical steps to help protect your data

## Minimise your data

- Data should be kept for no longer than is necessary. Over time you may have collected large amounts of data. Some of this data may be out-of-date and or no longer useful.
- Prevent unauthorised access by storing data which doesn't need regular access in a secure location.
- Delete data which you no longer need in line with your data retention and disposal policies.

# Practical steps to help protect your data

## Staff Awareness – IMPORTANT

- Communicate the Information Security Policy & Standards!! – **they are not internally confidential!!!!**
- Train your staff to recognise threats such as **phishing emails** and other malware or alerting them to the risks involved in posting information relating to your business activities on social networks
- **Joiners process** should include a security awareness module, managers should follow a **leavers process** and complete a checklist to ensure logical and physical access is revoked; and assets are returned (e.g. Removable Media, Storage Devices, Authentication Tokens etc.)
- Periodic Security Awareness Training to ensure staff are kept informed and up-to-date
- Keep your knowledge of threats up-to-date
  - Automated Information Sharing (**TAXII, STIX, CybOX**)
  - Vulnerability Datasource (**CVSS**)
  - Incidents (**VERIS**)
  - Information Sharing and Analysis Centre (Oil & Gas: **ONG-ISAC**, Multi-State (**MS-ISAC**))
  - Security Vendors (**Products and Services Patches**, Threat Intelligence (e.g. **IBM X-Force Threat Analysis Service**))
  - Vendor Led Sharing Alliances (e.g. **Cyber Threat Alliance**)
  - Open source (e.g. **IBM X-Force Exchange**)
  - Information Sharing and Analysis Organisations (**ISAOs**)
  - The Internet (Blogs (e.g. **Security Intelligence**), Podcasts (e.g. **CyberWire, SANS Internet Storm Center**, Social (e.g. **Twitter, LinkedIn**))



1 *Cyber attacks Trends*

2 *Threat Actors*

3 *Motivation of Threat Actors*

4 *Practical Steps to help Protect your Data*

5 **GDPR – So What?**

6 *In Summary*

# GDPR – An industry and geography agnostic regulation





# Prepare for GDPR – May 2018

## Preparing for the General Data Protection

### Regulation (GDPR) 12 steps to take now

1

#### Awareness

You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.

2

#### Information you hold

You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.

3

#### Communicating privacy information

You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.

4

#### Individuals' rights

You should check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.



5

#### Subject access requests

You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.

6

#### Lawful basis for processing personal data

You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.

7

#### Consent

You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.

8

#### Children

You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.

9

#### Data breaches

You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.

10

#### Data Protection by Design and Data Protection Impact Assessments

You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.

11

#### Data Protection Officers

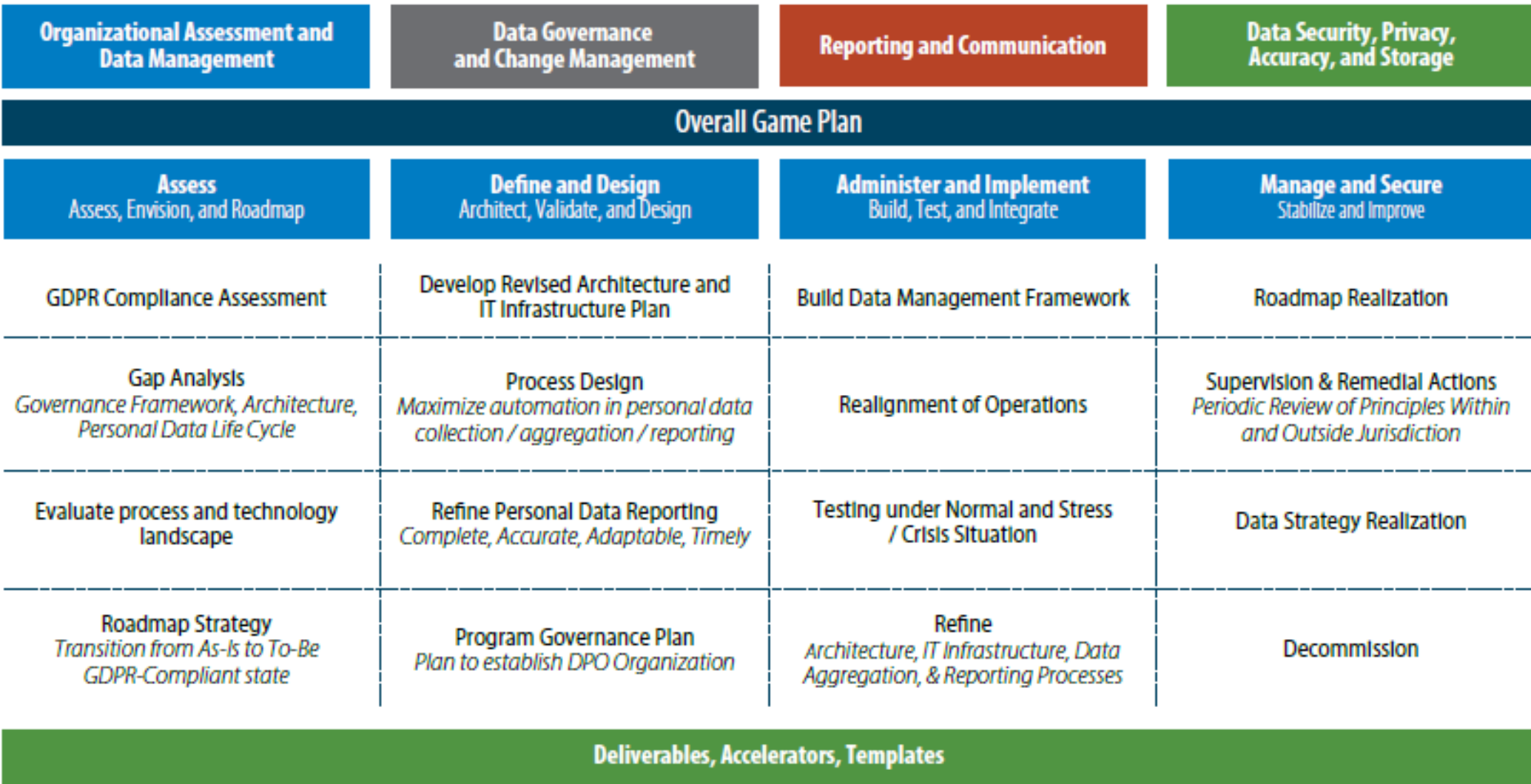
You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.

12

#### International

If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.

# Establish a GDPR Framework





- 1 *Cyber attacks Trends*
- 2 *Threat Actors*
- 3 *Motivation of Threat Actors*
- 4 *Practical Steps to help Protect your Data*
- 5 *GDPR – So What?*
- 6 *In Summary*



# In Summary

1. Cyber attacks and data breaches are not a case of **IF** but **WHEN!!**
2. Information & IT Security is not a cost, it's an **ESSENTIAL INVESTMENT**
3. **REVALIDATE and EVALUATE** where your current **investments** in security are being made
4. Review and update your **IT & Information Security Policies & Standards** on a periodic basis
5. Plan, Design, Implement and Maintain your **IT & Information Security Roadmap** and align to regulatory requirements such as GDPR
6. Implement and maintain a **Security Awareness Programme**

**You will sleep much better knowing you have done what you can do**



# Thank You



**Simon Tucker**  
**Partner**  
**Head of Energy Europe**  
**Tel: +447852211096**  
**Email: [simon\\_tucker@infosys.com](mailto:simon_tucker@infosys.com)**



**Vinnit Patel**  
**Senior Principal**  
**Head of Cybersecurity**  
**Tel: +447788 450825**  
**Email: [vinnit.patel@infosys.com](mailto:vinnit.patel@infosys.com)**

10 Upper Bank Street, 14th Floor, Canary Wharf  
London E14 5NP, United Kingdom  
Phone +44 20 7715 3300 | Fax +44 20 7715 3301