Housing Technology Conference 2016

Cyber Security

Building confidence in your digital future

pwc

Cyber attacks are headline news everyday

BBC Sign in News Sport Weather iPlayer TV

NEWS

Home UK World Business Politics Tech Science Health Education

Technology

Students hit by University of Greenwich data breach

By Leo Kelion
Technology desk editor

17 February 2016 | Technology

Association reports itself to ICO over data breach

9 November 2015 4:58 pm

Print | Email | Share | Comment | Save

A housing association has reported itself to the Information Commissioner after releasing tenants' private contact details.

Human Error Blamed For Increasing Number Of Data Breaches

South Wales Fire and Rescue Service staff data breached

9 February 2016 | South East Wales

The Register®
Biting the hand that feeds IT

DATA CENTRE SOFTWARE NETWORKS SECURITY INFRASTRUCTURE DEVOPS BUSINESS HARDWA

Security

Patient monitors altered, drug dispensary popped in colossal hospital hack

A dozen facilities fall as humble dropped USB sticks lead to network ruin

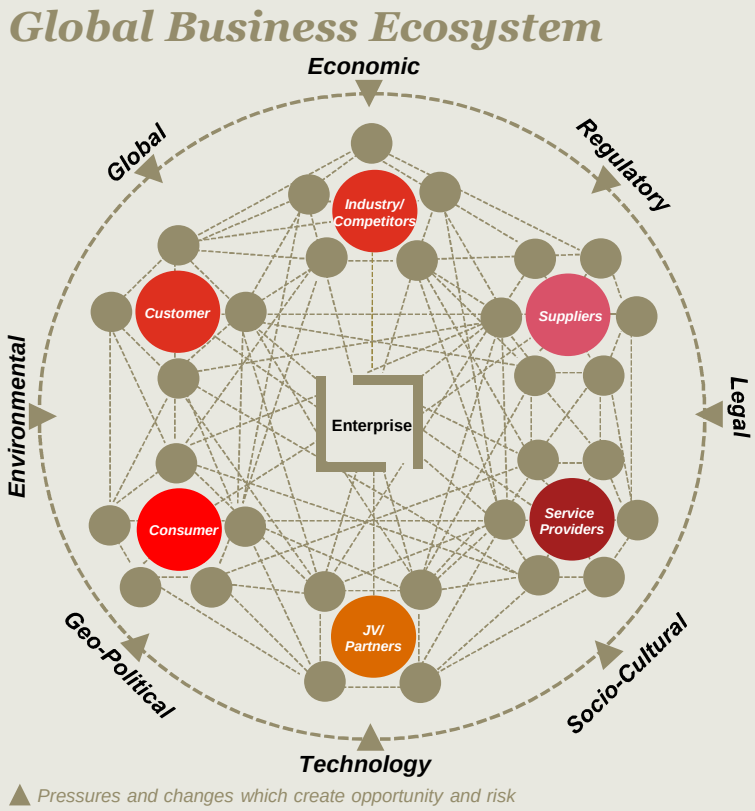
'Hack' on DoJ and DHS downplayed

A recent security breach highlights why social housing providers should consider how they handle data, say legal experts

The World Has Changed

Technology Use

We now operate in a global business ecosystem



Traditional boundaries have shifted; companies operate in a dynamic environment that is increasingly interconnected, integrated and interdependent.

- The ecosystem is **built around a model of open collaboration and trust**—the very attributes being exploited by an increasing number of global adversaries.
- Constant **information flow is the lifeblood of the business ecosystem**. Data is distributed and disbursed throughout the ecosystem, expanding the domain requiring protection.
- **Adversaries are actively targeting critical assets** throughout the ecosystem—significantly increasing the exposure and impact to businesses.

Years of underinvestment in security have impacted organisations' ability to adapt and respond to evolving, dynamic cyber risks.

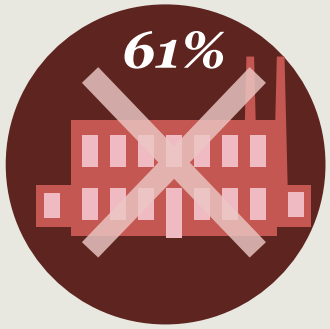
Cybersecurity is more than an IT challenge—it's a business imperative

48% increase in security incidents between 2013 and 2014. 42.8 million incidents reported (those that were detected!)

1 – 2015 PwC Global State of Information Security

Average losses are going up with the number of organisations reporting[2] losses of $20M or greater, increasing 34% from 2013.

2 – 2015 PwC Global State of Information Security



Per the Global CEO Survey, one-third of CEOs don't think a cyberattack would negatively impact their business. Yet 61% of consumers[3] would stop using a company's product or services if an attack resulted in a known breach.

3 – 2012 PwC Consumer Intelligence Series

Sources of cyber attacks

Nation State

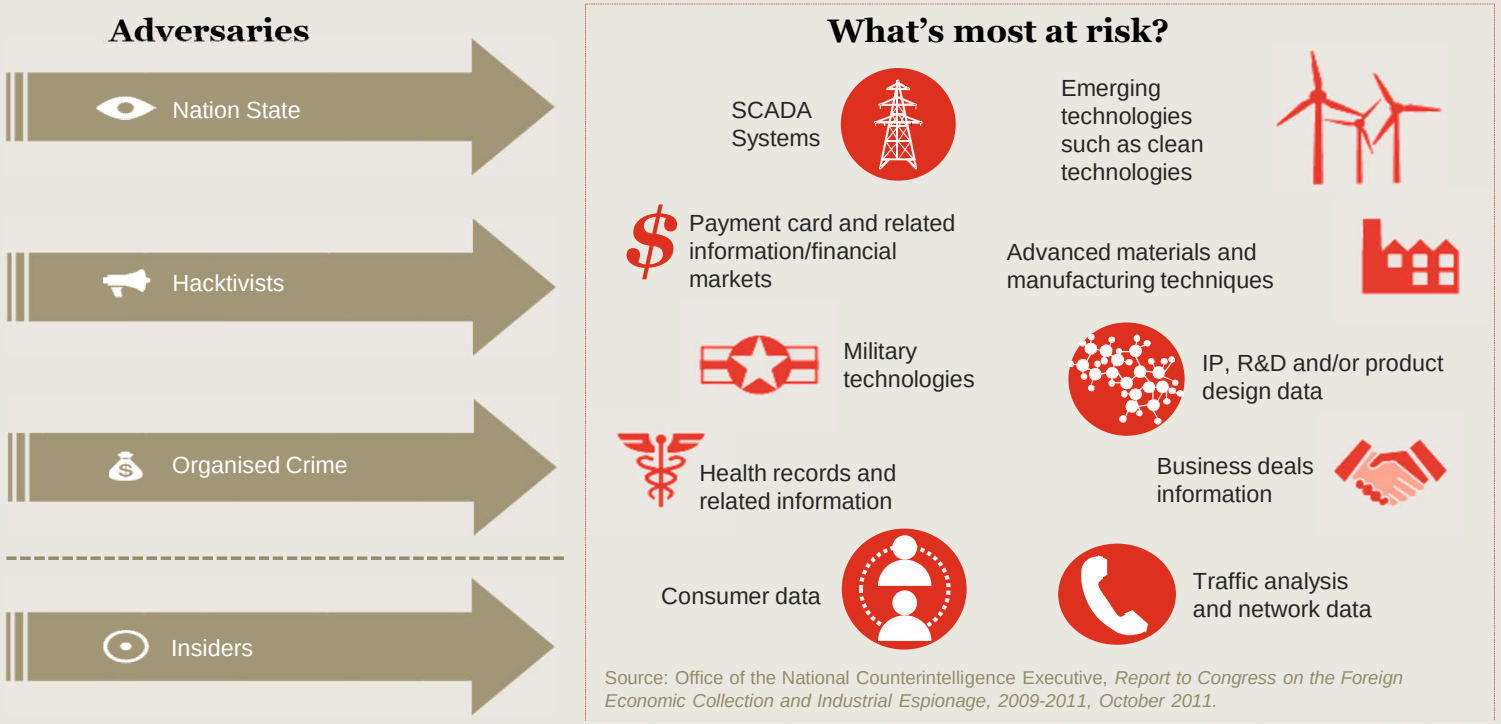
Hacktivism

[redacted]

Cyber Terrorists

Organised Crime

The information adversaries are after



Source: Office of the National Counterintelligence Executive, *Report to Congress on the Foreign Economic Collection and Industrial Espionage, 2009-2011, October 2011.*

Adversary motives ***evolve*** as business strategies change and business activities are executed; they can strike quickly, or they can be persistent and lie in wait; ***the assets most important*** to an organisation must be ***prioritised*** and ***protected*** first.

What is Cyber Security?

You can't secure everything

We help you set the right priorities

- Enterprise security architecture
- Protect what matters
- Strategy, organisation, governance
- Threat intelligence

It's not if but when

We help you build an intelligence-led defence, enabling rapid cyber response

- Continuity and resilience
- Crisis management
- Incident response
- Monitoring and detection

Fix the basics

We help you use technology to your advantage, deriving maximum return from your technology investments

- Identity and access management
- Information technology hygiene
- Information technology, operations technology and consumer technology
- Security intelligence and analytics

Seize the advantage

We help you exploit digital opportunity with confidence

- Compliance with privacy and regulation
- Digital trust is embedded in the strategy
- Risk management and risk appetite

Their risk is your risk

We help you understand and manage risk in your interconnected business ecosystem

- Digital channels
- Partner and supplier management
- Robust contracts

People matter

We help you build and maintain a secure culture, where people are aware of their critical security decisions

- Insider threat management
- People and 'Moments that Matter'
- Security culture and awareness

Protecting what matters

Protect the information that really matters

Effective security requires that you understand and adapt to changes in the threat environment by identifying your most valuable information.

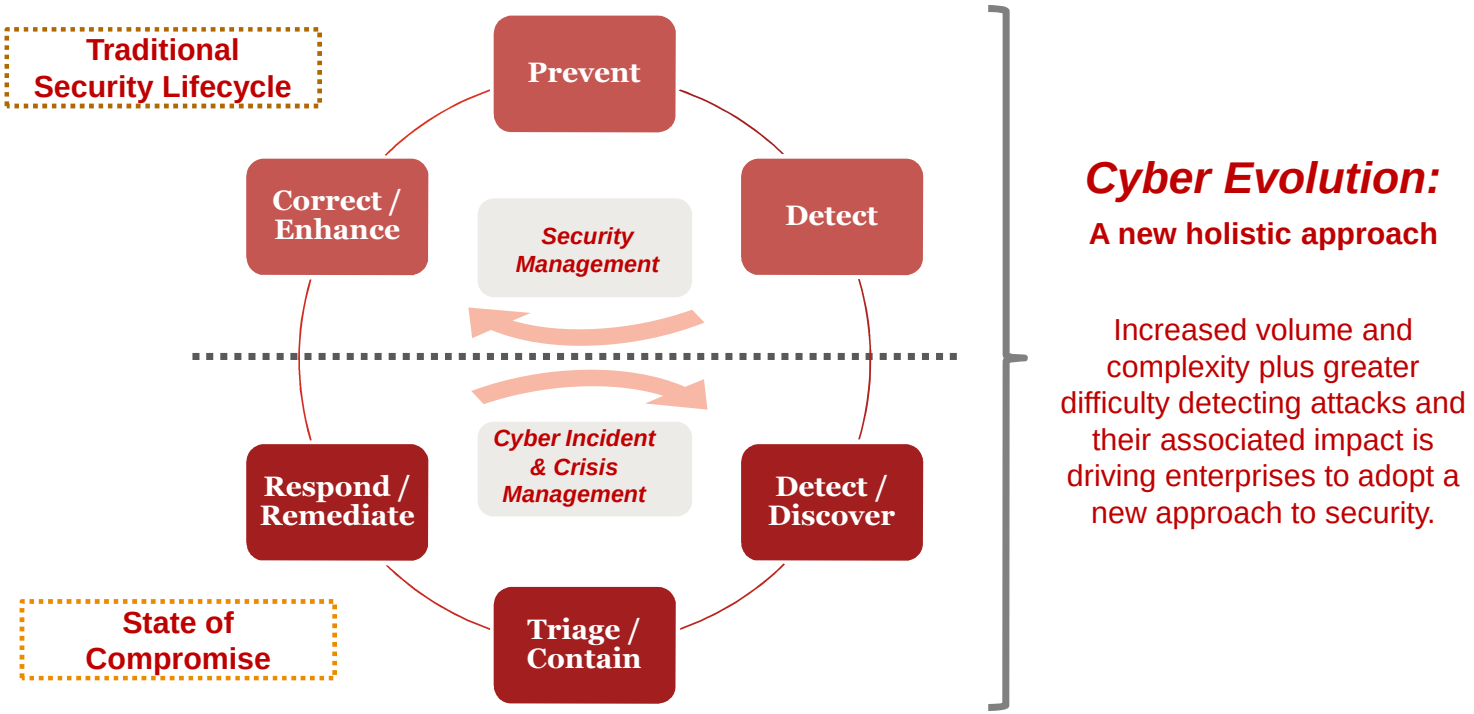
Know where these “crown jewels” are located and who has access to them at all times including third parties.

Understand how sensitive data moves around the business and externally.

Operating in an "Assumed State of Compromise"

Our clients are adjusting their security posture which anticipates a security breach/compromise has occurred or is underway.

They are evolving their approach to secure intellectual property and sensitive information with new and improved security capabilities.

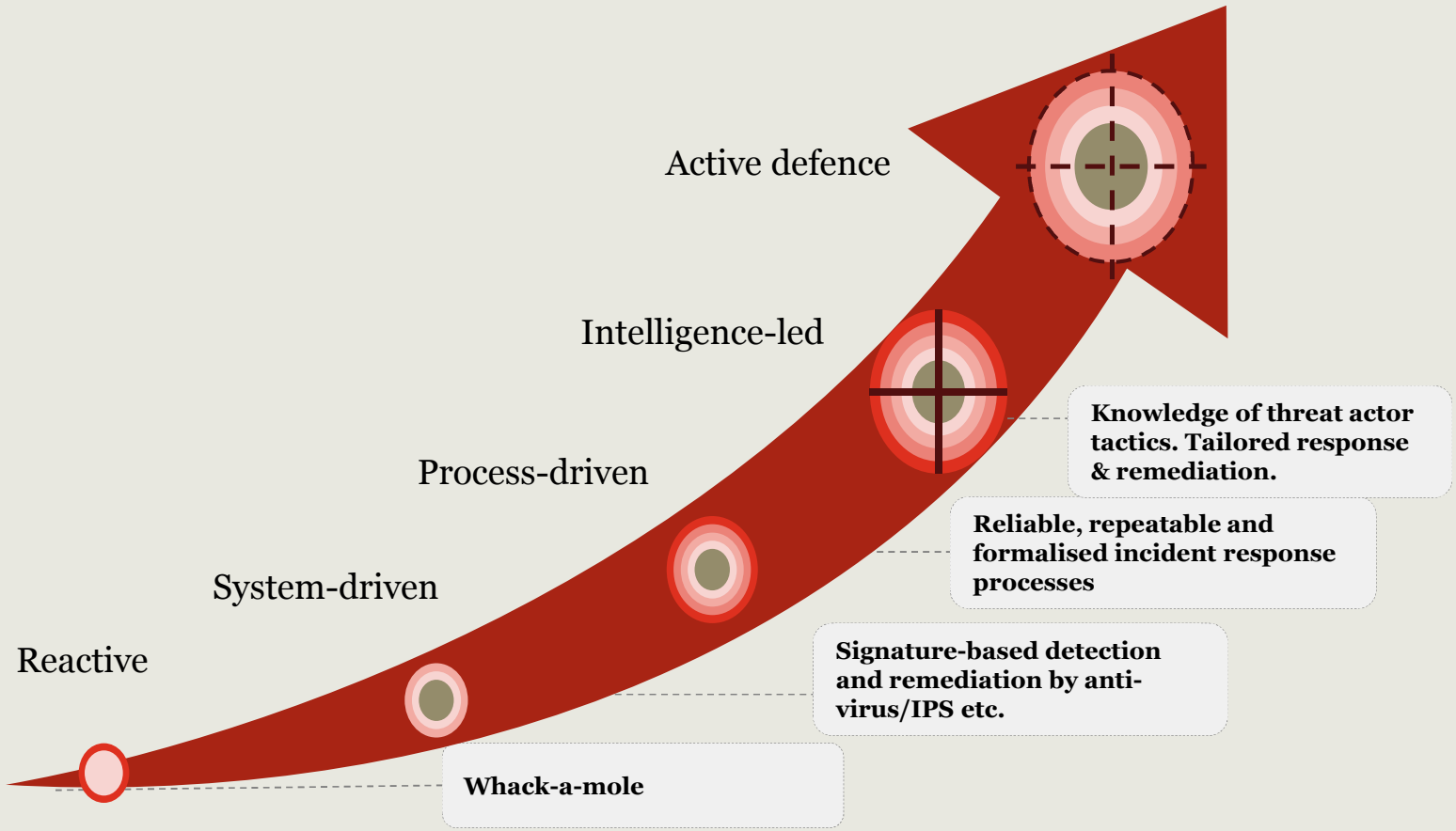


Cyber Evolution:

A new holistic approach

Increased volume and complexity plus greater difficulty detecting attacks and their associated impact is driving enterprises to adopt a new approach to security.

Incident response



Their risk is your risk

Do they have a good security culture? ISO27001?

Do they process sensitive data on your behalf?

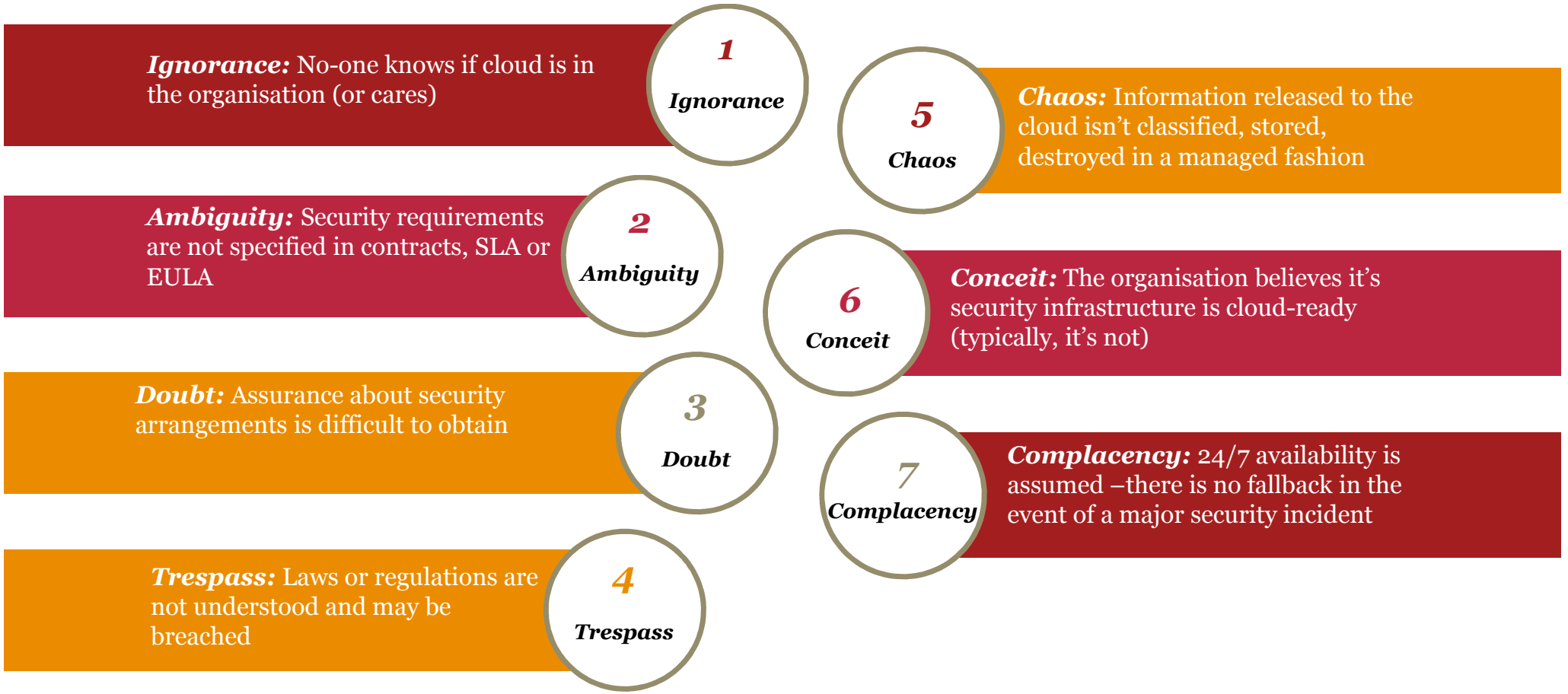
Robust contracts – do they specify the controls you would expect to see implemented over your data

Do you perform Due Diligence on new suppliers

Do you have the right to audit / perform security testing?

Joined up incident response? Are they a true partner?

7 Deadly Sins of Cloud Computing



People

Embedded security culture

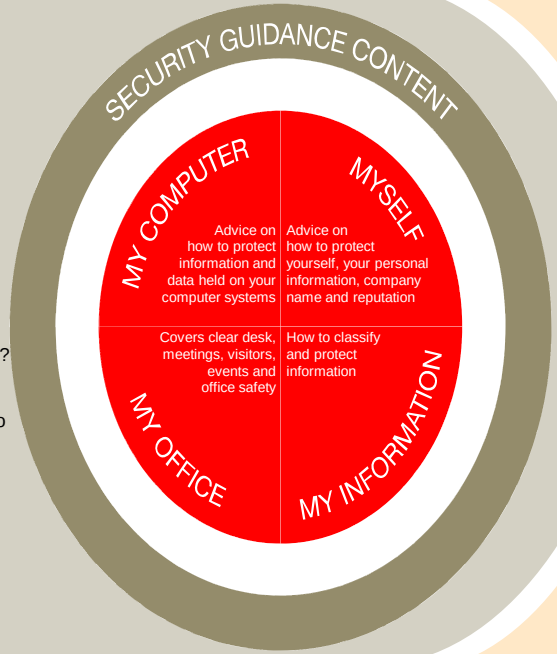
Have you identified the moments that matter?

Organisational culture and governance

- To what extent does the culture of the organisation support or obstruct good security behaviours?
- Who is accountable for security performance and do they have the authority and resources they need?
- How is security performance measured, good behaviour rewarded and poor behaviour sanctioned?

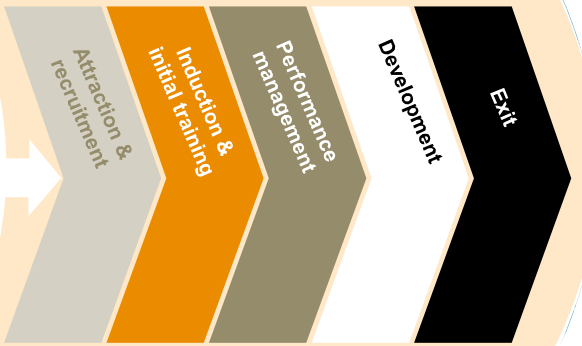
Communications strategy

- Do you have effective communication channels and are you using them through the full employee life cycle?
- Can you provide regular updates and other 'triggers' to point staff at security guidance content?
- What do you want your staff to know, think and do and how will you deliver these outcomes?



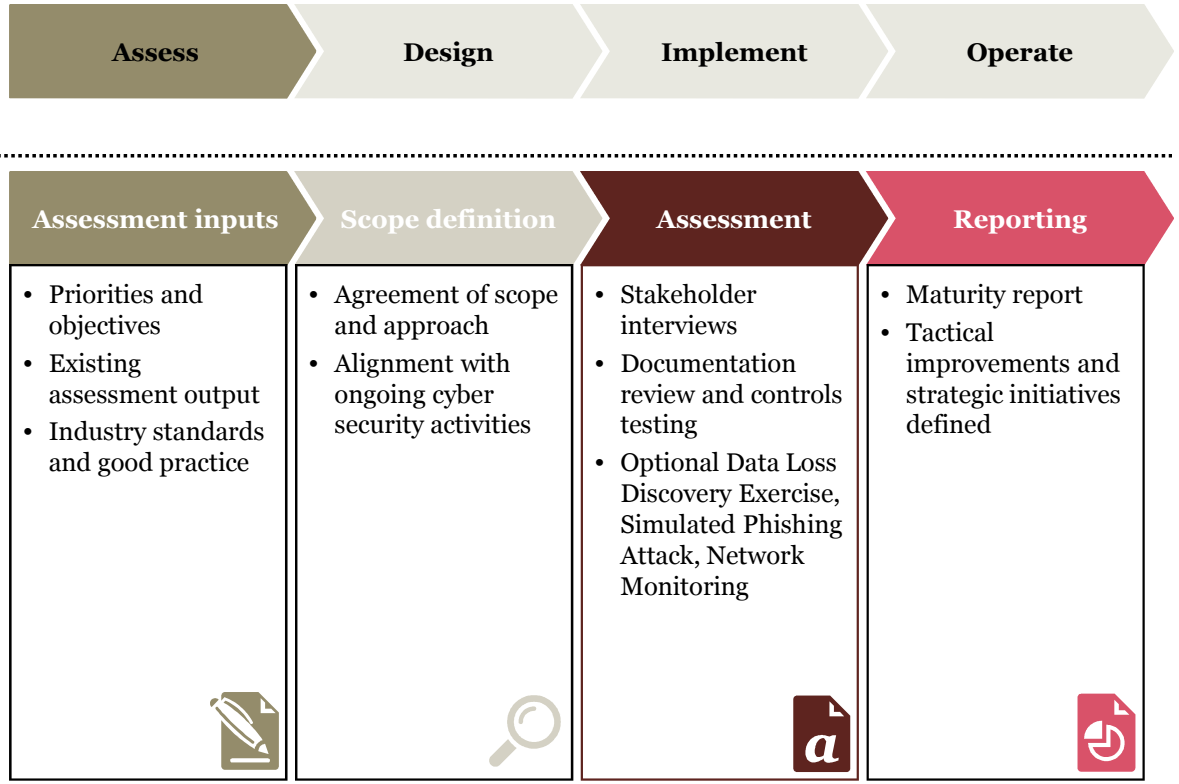
Employee lifecycle events

- How people processes re-inforce the information security standards



Making a start – Gap Analysis

As with all effective programmes there needs to be distinct phases to ensure success.



EU General Data Protection Regulation

After four long years of political negotiations and lobbying, the EU has finally adopted the "General Data Protection Regulation" (GDPR). This will impact every entity that holds or uses European personal data both inside and outside of Europe.

This landmark legislation will gives rise to increased compliance requirements backed by heavy financial penalties (*up to 4% of annual worldwide turnover for groups of companies*). Entities will have only two years from the adoption of the GDPR to implement all the necessary changes to their systems and operations to meet the new compliance requirements.

Your organisational strategy and approach to comply with the GDPR will need to encompass the **three key components** reflected within the regulation:

- a new compliance journey;
- a new transparency framework; and
- a new enforcement, sanctions and remedies framework.

EU General Data Protection Regulation

Compliance

The new ***compliance journey*** will require entities to:

- map and classify all their personal data
- perform risk assessments
- design privacy protections into all new business operations and practices
- employ dedicated Data Protection Officers
- monitor and audit compliance
- document everything that they do with data and everything they do to achieve legal compliance.

Transparency

The ***new transparency framework*** will require entities to re-think:

- how they engage with people, including their contracting and permissions processes
- how they give clear and full information on what's happening to personal data.

When a breach of security or confidentiality arises, entities will have to notify the incident to the regulators. In serious cases they will have to notify the people affected.

Legal risk

The ***new enforcement, sanctions and remedies framework*** will give regulators:

- unprecedented powers to intervene in business and to shape how entities conduct their operations
- powers to impose very heavy fines (up to 4% of annual worldwide turnover for groups of companies).

Individuals will:

- be able to exercise a new "right to be forgotten“ and a new "right of data portability"
- have enhanced rights of access to their data and to demand the end of use of their data
- be able to sue entities for compensation, if they are distressed by acts of non-compliance.

Q&A

Neil Ward
Senior Manager
neil.j.ward@uk.pwc.com