Managed Services & Consultancy – Providing Essential Skills & Resource

A Presentation of Two Halves

As you can tell I am not Dave!

Earthquakes, Asperities & Tsunami's

Threat landscape

Attackers + Punitive Regulation + Material Fines = Instability

Are we back to the good old days of extortion, racketeering and protection money?
Just brought bang up to date on delivery method?

Threat horizon

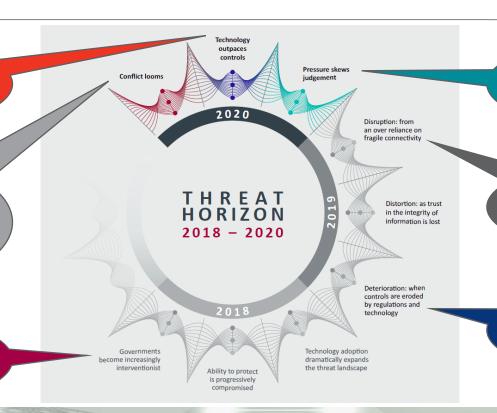**BYTES** SECURITY PARTNERSHIPS

Artificially intelligent malware amplifies attackers' capabilities

Chinese hackers compromise satellites using privileged accounts (last week)

Weaponised IoT

Disruptive companies provoke governments into legislating

GDPR / NIS case law & fines cause knee jerk, increasing compliance burden

Premeditated internet / company outages bring trade to its knees

See 'My conversation with the ICO!' (later in my slides)

Adapted from the ISF

Technology outpaces controls

Conflict looms

Pressure skews judgement

2020

Disruption: from an over reliance on fragile connectivity

THREAT HORIZON 2018 – 2020

2019

Distortion: as trust in the integrity of information is lost

Deterioration: when controls are eroded by regulations and technology

2018

Governments become increasingly interventionist

Ability to protect is progressively compromised

Technology adoption dramatically expands the threat landscape

Why is security failing?

Scoping

Business Impact Assessment

Threat Profiling

Vulnerability Assessment

Risk Evaluation

Risk Treatment

Adapted from the ISF

My conversation with the ICO!

- [Me]..I have a customer that uses biometric clocking systems for identification and authentication, how do we process this special category of data lawfully, as none of the options in Article 9 seem to fit?

- [ICO]..We only enforce the legislation we do not make the policy, but you can always refer this to your MP if you wish the law to be revised;

- [Me]..Well thanks that is helpful (ED: Not!), so what about lawful processing?

- [ICO]..Biometric clocking devices are not specifically covered by the GDPR or DPA2018 but the data that they use is;

- [Me]..Yes I know, and there is no clear guidance in the GDPR/DPA2018 and you have no specific information or anything from the WP29, that is why I phoned you!

- [ICO]..Well the issue is that you have other options that are available and you do not need to use biometrics data;

- [Me]..Yes, but my customer has suffered fraud using cards and fobs, and they need to comply with Working Time Directive. We have issues with using explicit consent as you say that it is incompatible for employment purposes;

- [ICO]..Yes, I understand but my Gym has biometric access and I am happy to consent for its use;

- [Me]..This is somewhat different as it is not in relation to your employment;

- [ICO]..Well then your only option is to decide on a legal basis for processing that we will not object to, or you must take the system out, I will leave that to you to explain to your customer;

- [ICO]..Remember that your rights as an employer and your requirements as a business should not override the rights and freedoms of individuals as these are more important.

So what does this all mean?

Over the coming years, the very foundations of todays digital world will shake - violently. [ISF]

By 2020, 60% of digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk. [Gartner]

Most realistic CISO's accept the fact that breach is now inevitable. [Me]

Data breaches are often discovered long after they occurred. Ponemon Institute's 2017 Cost of Data Breach Study for the UK found that it takes organisations an average of 191 days to identify a data breach and 66 days to contain it. The longer it takes to identify and contain a breach, the more it costs. [Ponemon]

Half time oranges!

What should we do?

Adapted from the ISF

A IDENTIFY mission-critical information assets

B ASSESS the main adversarial threats

C DETERMINE the required protection approaches

D COUNTER the main adversarial threats

E PROTECT the information life cycle

Advisory Consulting

Product and Solution

Assurance & Audit
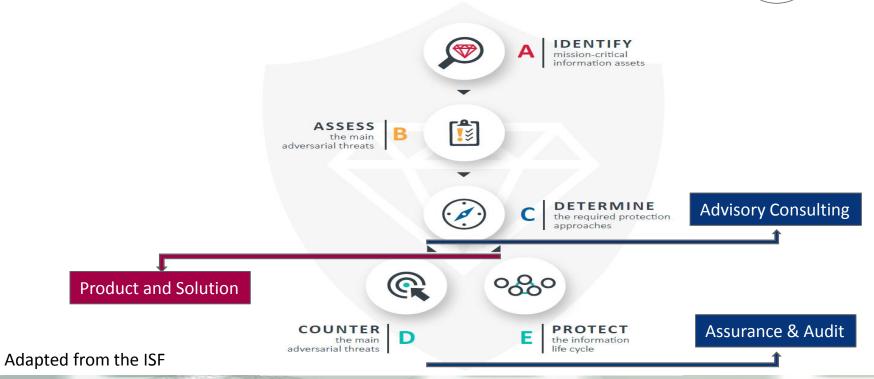
So that's great, how do we do it?

Governance, Risk and Compliance (GRC)
Set direction for security, promote ownership, collaborate with stakeholders.

People
Invest in skilled and experienced IT practitioners, security specialists and risk experts.

Technology
Automate protection of mission-critical information assets using security architecture, specialised technical security controls and advanced security solutions.

Security Assurance
Provide assurance for the protection of mission-critical information assets.

What do we offer?

Security Consulting

(Advisory Consulting Services)

Phoenix Software

(Software, Solutions and IT)

Software Services

(Software and Licensing)

Security Partnerships

(Security Solutions including Managed SOC)

Security Consulting

(Audit and Assurance i.e. Pen Testing)

2018: GDPR, PCI, ISO27001, Information Security & ISF, Risk and Penetration Testing

My final thoughts!

🌀 [Captain Blackadder]..Can anyone tell me what's going on?

🌀 [Captain Darling]..Security, Blackadder.

🌀 [Captain Blackadder]..Security?

🌀 [General Melchett]..Security isn't a dirty word, Blackadder. Crevice is a dirty word, but security isn't.

🌀 [Captain Blackadder]..So in the name of security, sir, everyone who enters the room has to have his bottom fondled by this drooling pervert?

🌀 [Captain Darling]..I'm only doing my job, Blackadder.

🌀 [Captain Blackadder]..Well, how lucky you are then that your job is also your hobby.

©BBC

As Always, Dave has the last word!

"As Steve has said breaches are inevitable. Monza told Ticketmaster in April that something was wrong. Ticketmaster initially ignored them and didn't let customers know until yesterday. Don't be that kind of business