Latest GDPR news and Cyber Security as a Service (CSaaS)

Presented by:

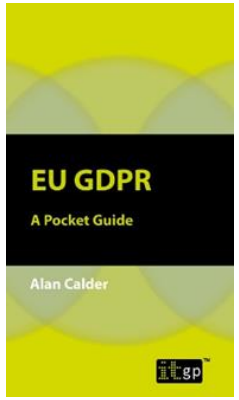
- **Alan Calder, Founder and Executive Chairman, IT Governance**

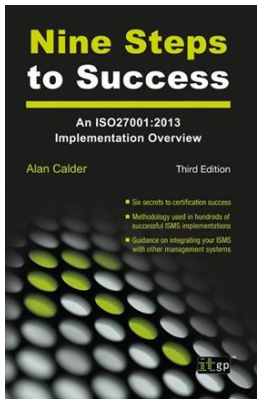
27 November 2019

Introduction

Alan Calder

- Founder and executive chairman of IT Governance.
- IT Governance is the leading global provider of IT governance, risk management and compliance solutions.
- Author of *IT Governance – An International Guide to Data Security and ISO27001/ISO27002* and *EU GDPR, A Pocket Guide.*





Protect • Comply • Thrive

AMCA: A breach and its context

40 years in business: never had a data breach

2015: Spent $1 million to upgrade and modernise IT Infrastructure

What's to worry about?

Hackers accessed its systems in 2018

Went undiscovered for 7 months

Exfiltrated detailed personal records of 20 million US citizens

Hack discovered by a third party

$400k with 3 cyber security companies to bolt the door

Owner injected $2.5 million for data breach notifications

Main customers terminated contracts, victims launched class action suit

Fired 80% of its staff

Filed for bankruptcy protection on 19 June 2019, preparatory to liquidation.

AMCA: American Medical Collections Agency

AMCA: Lessons?

Spending $200k on active cyber security would be better than throwing $400k at the stable door

Cyber insurance is not an adequate defence

The past is not a guide to the future

Cyber security has to be pro-active, up-to-date and agile

Directors have to make themselves personally accountable for cyber security

Source: Verizon, 2019 Data Breach Investigations Report

Major fresh produce wholesaler

70 years in business: never had a data breach

Independent IT infrastructure in each OPCO/region – but much not updated

£1 Million in Cyber breach cover

What's to worry about?

Successful EMOTET attack via a phishing email

Self-replicated across the Group

Released ransomware onto main group systems

Cyber insurer identified EMOTET but couldn't deploy resource

IT Team never had to deal with ransomware and overwhelmed by internal cries for help

No business continuity plans, no network diagrams, no asset records, and backups also infected

GDPR Compliance no longer up-to-date

Resorted to paper and pen for daily operations

Rebuilt and restored network from ground up.

Recovery costs nearing £5m million

AMCA: American Medical Collections Agency

EMOTET: Lessons?

It's better to invest in secure infrastructure before an attack than afterwards

Cyber insurance is not an adequate mitigation

Internal teams are not trained to handle or respond to cyber attacks

The past is not a guide to the future

Cyber security has to be pro-active, up-to-date and agile

Directors have to make themselves personally accountable for cyber security

Source: Verizon, 2019 Data Breach Investigations Report

The nature and impacts of cyber threats

16% were breaches of **public sector entities**

15% were breaches involving **healthcare organisations**

10% were breaches of the **financial industry**

43% of breaches involved **small businesses**

71% of breaches were **financially motivated**

25% of breaches were motivated by the **gain of strategic advantage**

32% of breaches involved **phishing**

29% of breaches involved **use of stolen credentials**

Source: Verizon, 2019 Data Breach Investigations Report

GDPR-readiness is a good thing!

59% reported compliance with all or most of GDPR's requirements; **29%** expecting to get there within a year

Less likely to have experienced a data breach in the last year (74% vs. 89%)

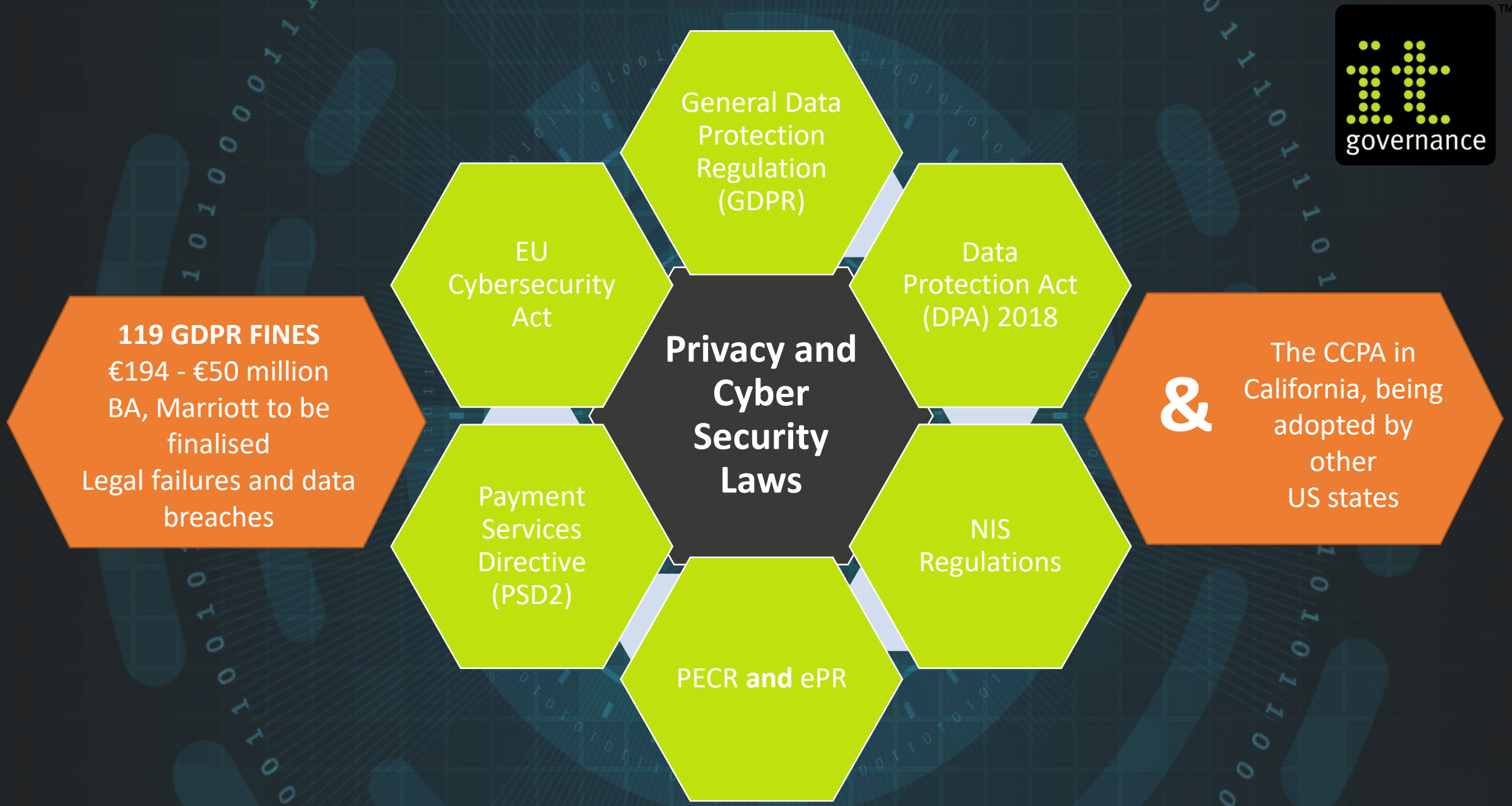
Shorter sales delays due to customer's privacy concerns (3.4 vs. 5.4 weeks).

Lower data breach costs only 37% vs. 64% of the least GDPR ready had a loss of over $500,000 last year

Fewer records breached (79k vs. 212k records)

Shorter system downtime (6.4 vs. 9.4 hours)

Source: CISCO CYBERSECURITY SERIES 2019 Data Privacy Benchmark Study


General Data Protection Regulation (GDPR)
EU Cybersecurity Act
Data Protection Act (DPA) 2018
Privacy and Cyber Security Laws
Payment Services Directive (PSD2)
NIS Regulations
PECR and ePR
119 GDPR FINES
€194 - €50 million
BA, Marriott to be finalised
Legal failures and data breaches
&
The CCPA in California, being adopted by other US states

Cyber security scarce skills

70% said the cybersecurity skills shortage had impacted their organisation (ESG & ISSA Research Report: The Life and Times of Cybersecurity Professionals 2018)

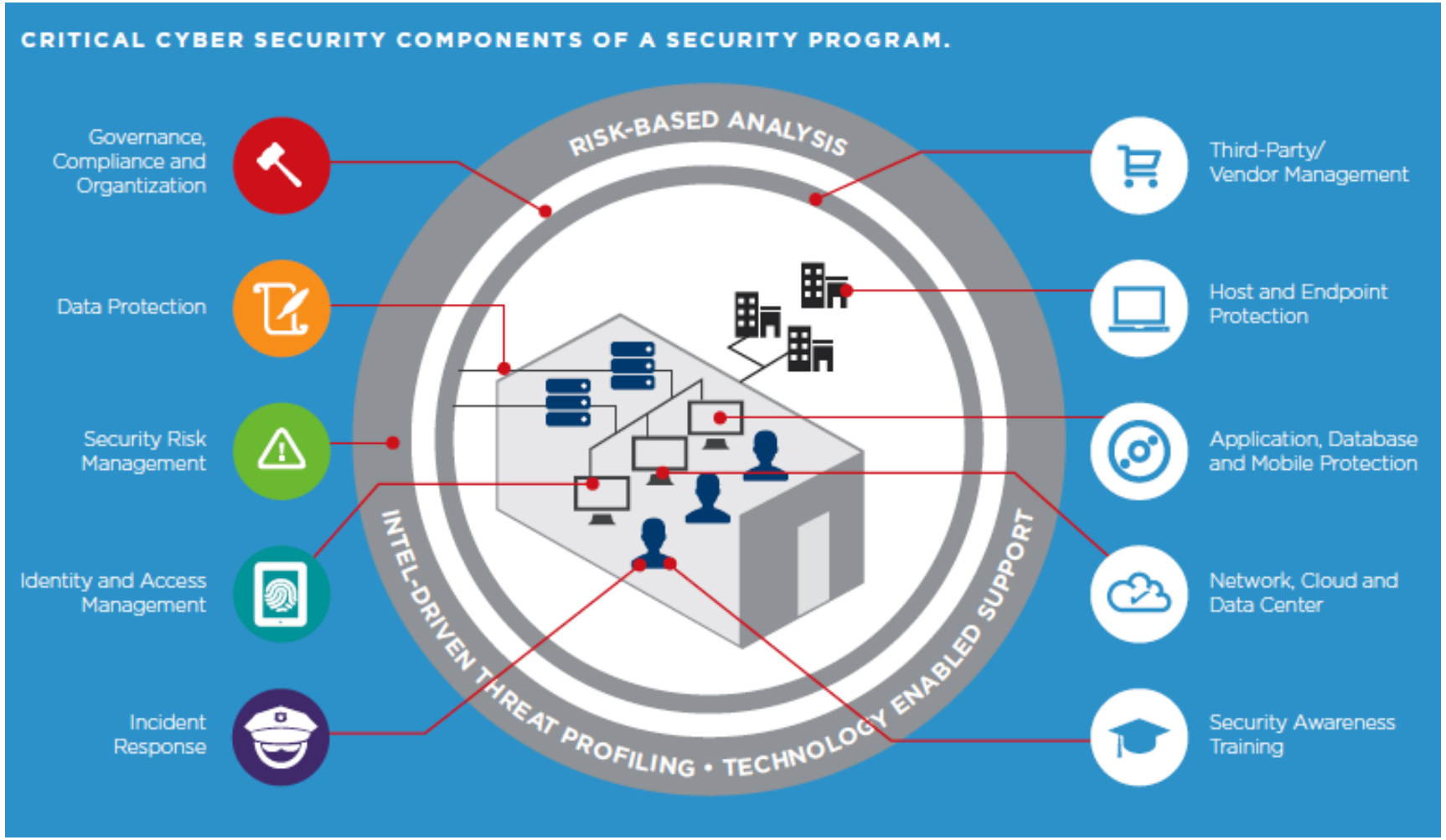
47% of respondents claim that the cybersecurity skills shortage has resulted in an inability to fully learn or utilize some security technologies to their full potential. (ESG annual cyber security survey)

82% of employers surveyed in 8 countries report a shortage of cyber security skills (Hacking the Skills Shortage, McAfee/CSIS)

71% believe this talent gap causes direct and measurable damage to their organisation (Hacking the Skills Shortage, McAfee/CSIS)

Women make up only 14% of the US cyber security workforce

Critical elements of a cyber security team



Source: Mandiant https://www.fireeye.com/services.html

Cyber Security as a Service (CSaaS)

Addresses all aspects of information and cyber security, governance, risk management and compliance

One agreement with one trusted partner

Bring on board resources quickly and only when required

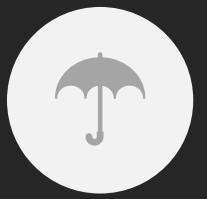
Eliminate the need to attract and retain expensive talent

Lower costs without compromising on security

Let’s you get on with running the business!

Cyber Security as a Service (CSaaS)

Cyber security risk assessment



Managed protection

Response and recovery

Governance and assurance

Let’s you get on with running the business!

How to get in touch with us

Visit our website
www.itgovernance.co.uk

Email us
servicecentre@itgovernance.co.uk

Call us
+44 (0)333 800 7000

Join us on LinkedIn
/company/it-governance

Like us on Facebook
/ITGovernanceLtd

Follow us on Twitter
/itgovernance

Questions

Protect • Comply • Thrive