ISACA®
Trust in, and value from, information systems
Harare Chapter

BIG DATA AND ANALYTICS SECURITY, PRIVACY AND GOVERNANCE

11 September 2018

ISACA®
Trust in, and value from, information systems

SUMMARY OVERVIEW

EVERYTHING IS DATA BUT CAN EVERYTHING BE SECURE

IT'S BIG BECAUSE…

'Big data is big because of a high level of volume, velocity and variety'

Source: Implementation of Big Data in Commercial Banks

Adeniyi Akanni, Ph. D., CISA, CRISC, ITIL -ISACA Volume 1, 2018

SECURITY

VOLUME-VELOCITY-VARIETY

Makes you ask questions

1. Where is the security points
2. What is the best way to be secure
3. Who can be trusted in this interchange
4. How is the source defined and controlled

Source: http://archive.climateplan.org/caltrans-get-times/ (By Maya Wallace, ClimatePlan Communications & Network Director)

WHERE IS THE PRIVACY

Data Protection Directives (DPD) definition of “Personal data is personal information relating to an identified or identifiable natural person”

What can we use to identify you? Is it secure

THE 3 V MODEL

Volume—Refers to the "bigness" of big data.

Velocity—Refers to the speed at which data are generated and/or changed.

Variety—Refers to the multiple sources and types of data that may be employed in a big data solution.

veracity, value, variability and visualization

Veracity

Lastly, big data has to be of some value to your organization. In order to be of value we have to make sure that it is correct.-https://www.admintome.com/blog/big-data-examples/

Is Your Organisation aware of its 3 V Model

WHERE YOUR ORGANISATION FITS

1 Minute Statistics-2018 by Forbes

- We send 16 million text messages
- 156 million emails are sent; worldwide it is expected that there will be 9 billion email users by 2019
- 15,000 GIFs are sent via Facebook messenger
- Every minute there are 103,447,520 spam emails sent
- There are 154,200 calls on Skype
- Uber riders take 45,788 trips!
- Users watch 4,146,600 YouTube videos

Source https://www.forbes.com/sites/bernardmarr/2018/05/21/how-much-data-do-we-create-every-day-the-mind-blowing-stats-everyone-should-read/#184bb5d460ba

WHERE IS YOUR SECURITY

Veracity – 27% of businesses are not sure if the data they are working on is accurate.-Gartner

Incident	Impact
Yahoo **Date:** 2013-14	**Impact:** 3 billion user accounts
Adult Friend Finder **Date:** October 2016	**Impact:** More than 412.2 million accounts
eBay **Date:** May 2014	**Impact:** 145 million users compromised
Heartland Payment Systems **Date:** March 2008	**Impact:** 134 million credit cards exposed through SQL injection to install spyware on Heartland's data systems.

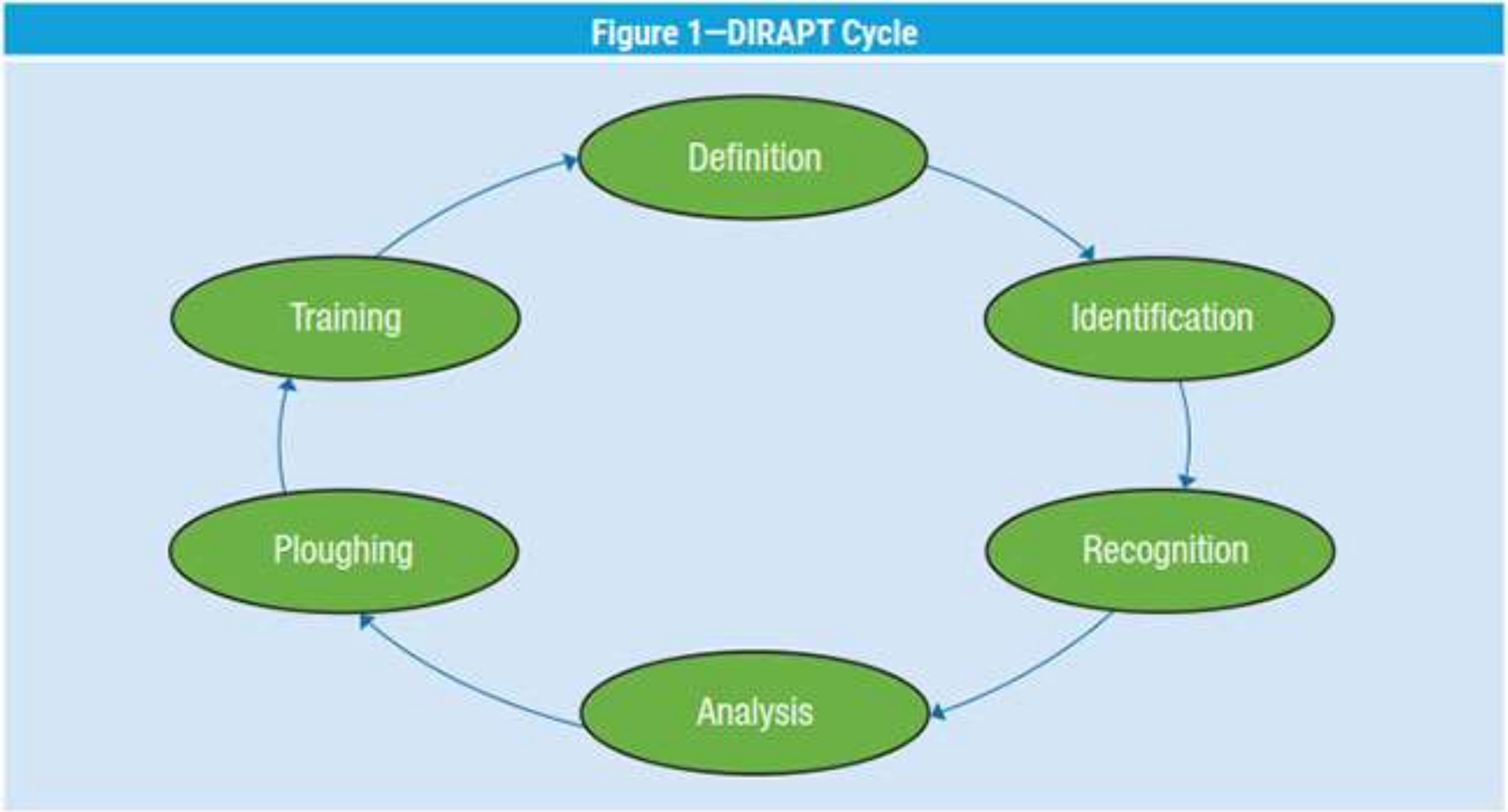
https://www.csoonline.com/article/2130877/data-breach/the-biggest-data-breaches-of-the-21st-century.html

Source: https://intellipaat.com/blog/7-big-data-examples-application-of-big-data-in-real-life/

WHERE IS YOUR SECURITY

If eBay, Yahoo and others can be compromised then us?

IMPLEMENTING SECURITY



Source: https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/implementation-of-big-data-in-commercial-banks.aspx

IMPLEMENTING SECURITY

#	Method	Description
1	**Definition of Scope**	Define your boundaries
2	**Identification of Skill Set**	Identify who is going to work wit the big data challenge. Include as many departments as possible.
3	**Recognition of Data Sources**	Identify and list each source
4	**Analysis of Output**	Analyse for value
5	**Ploughing Back Experience**	Use experience and lessons learned for the future
6	**Training and Retraining**	Development of the human mind is neccessary

DEIDENTIFICATION, REIDENTIFICATION AND ANONYMIZATION

- ***Deidentification*** is the altering of personal data to establish an alternate use of personal data so it is next to impossible to identify the subject from which the data were derived.

- ***Reidentification*** is the method of reversing the deidentification by connecting the identity of the data subject

- ***Anonymization*** is the ability for the data controller to anonymize the data in a way that it is impossible for anyone to establish the identity of the data.

https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/big-data-deidentification-reidentification-and-anonymization.aspx

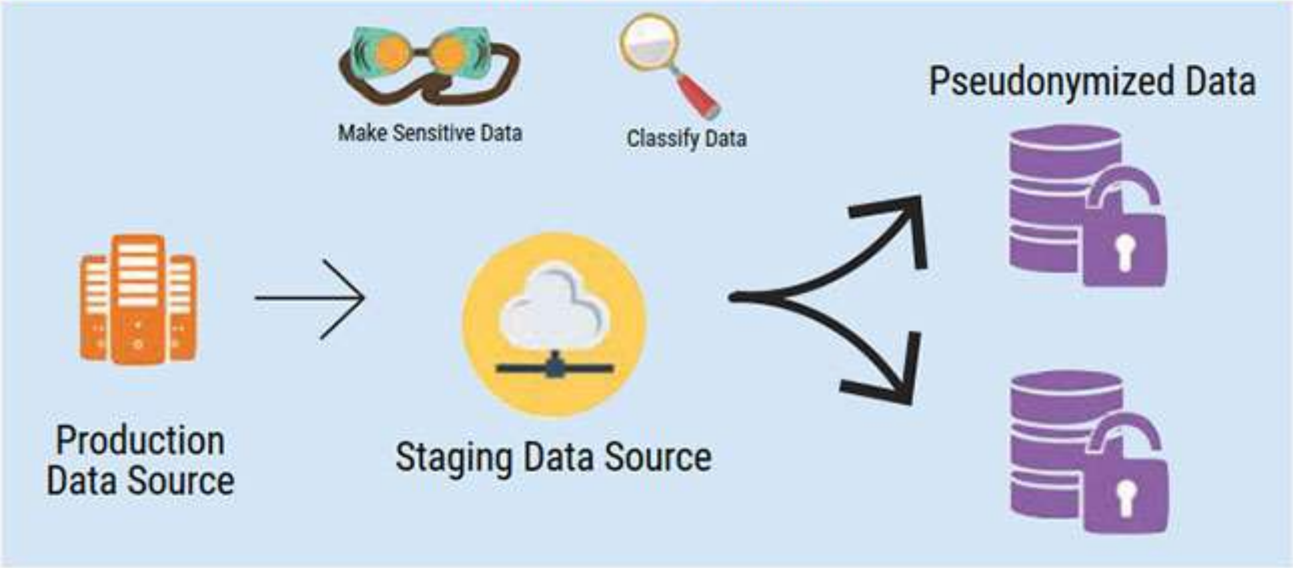
PSEUDONYMIZING AND ANONYMIZING DATA

Pseudonymization is the process of deidentifying data sets by replacing all identifying attributes, that are particularly unique (e.g., race, gender) in a record with another

- Eliminating the ability to connect data sets to other data sets, making identification of anonymized data uniquely identifiable
- Storing the encryption key securely and separately from the encrypted data
- Data protection using administrative, physical and technical security measures

https://www.isaca.org/Journal/archives/2018/Volume-1/Pages/big-data-deidentification-reidentification-and-anonymization.aspx

Figure 3—Pseudonymization



PSEUDONYMIZING AND ANONYMIZING DATA

Anonymization is essentially the destruction of identifiable data; therefore, it is virtually impossible to re-establish the data together.

Techniques to Anonymize

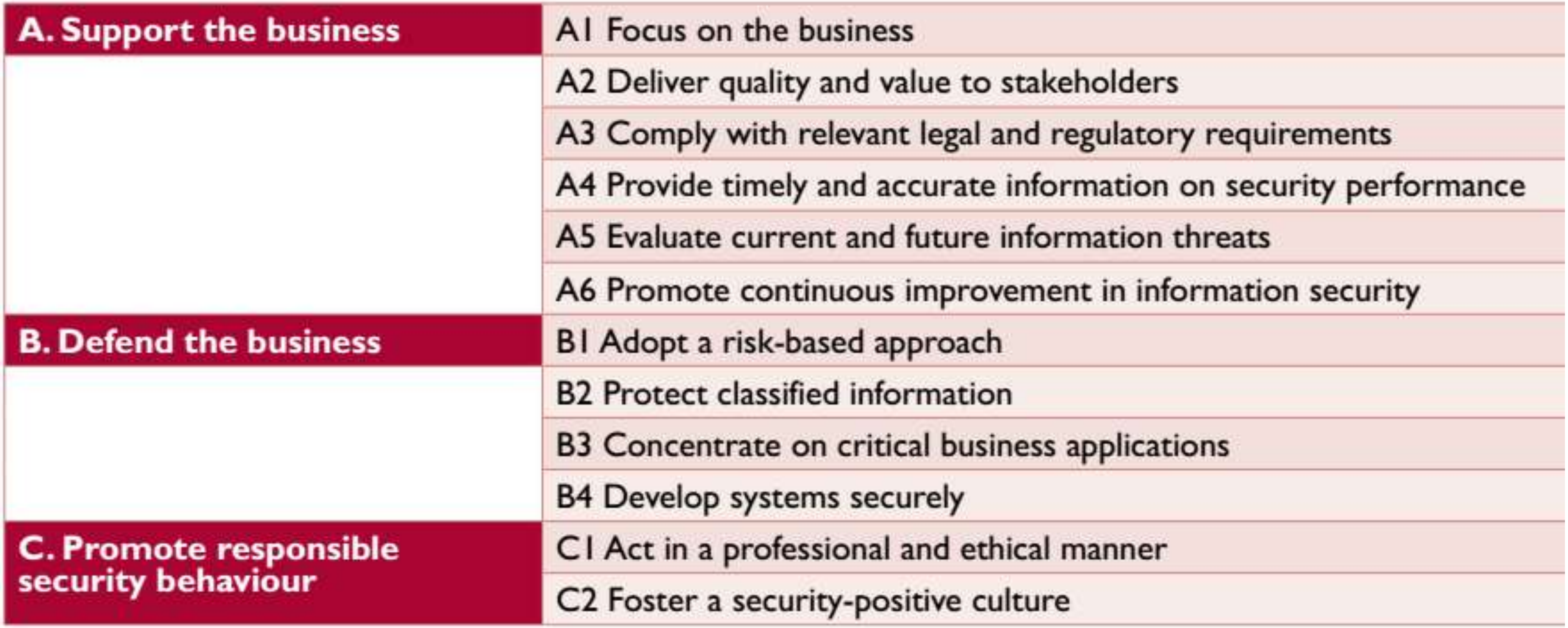
Generalisation: Grouping all data but no specific identification

Randomisation

- **Noise addition**—Alters the attributes by adding or subtracting a different random value for each record (e.g., adding a different random value between A+ and C- for the grade of the data subject)

- **Permutation**—Consists of swapping the values of attributes from one data subject to another (e.g., exchanging the incomes of data subjects with failed grades of data subject A with data subject B)

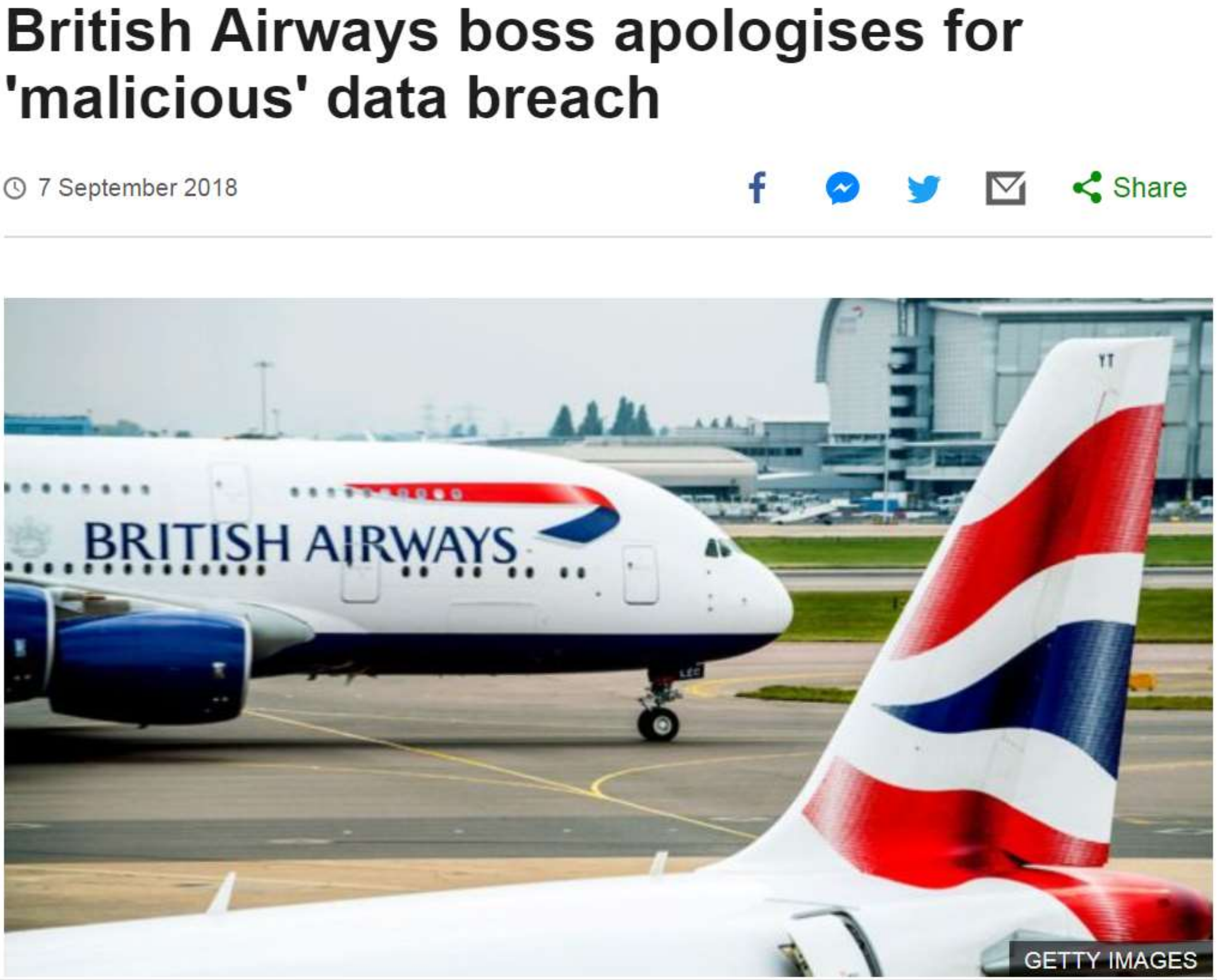
12 PRINCIPLES TO THINK OF



A. Support the business	A1 Focus on the business
	A2 Deliver quality and value to stakeholders
	A3 Comply with relevant legal and regulatory requirements
	A4 Provide timely and accurate information on security performance
	A5 Evaluate current and future information threats
	A6 Promote continuous improvement in information security
B. Defend the business	B1 Adopt a risk-based approach
	B2 Protect classified information
	B3 Concentrate on critical business applications
	B4 Develop systems securely
C. Promote responsible security behaviour	C1 Act in a professional and ethical manner
	C2 Foster a security-positive culture

Principles for Information Security Practitioners are reproduced with the permission of the Information Security Forum (ISF) for use by representatives of (ISC)² and ISACA

CASE STUDY: BRITISH AIRWAYS APOLOGIES



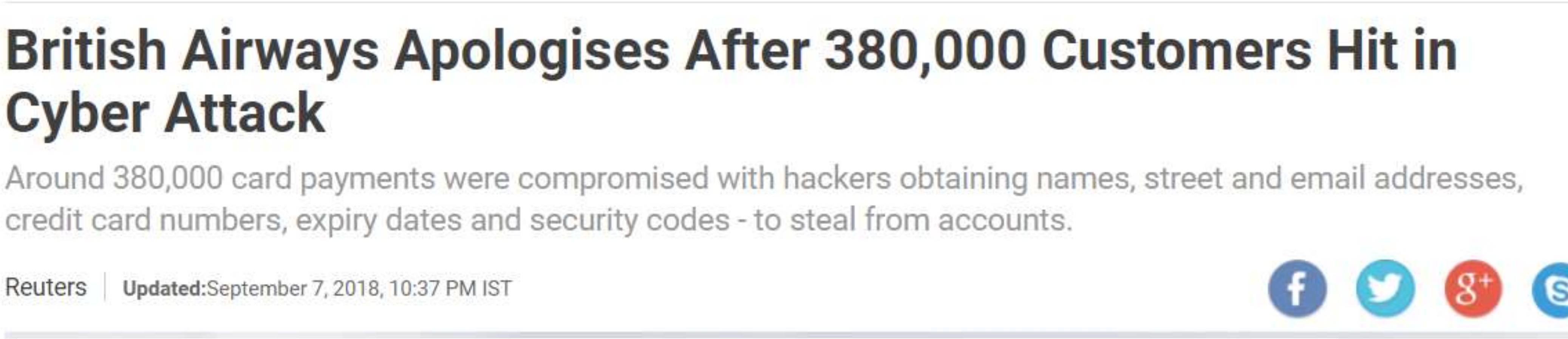
British Airways boss apologises for 'malicious' data breach

7 September 2018

GETTY IMAGES

https://www.bbc.com/news/uk-england-london-45440850

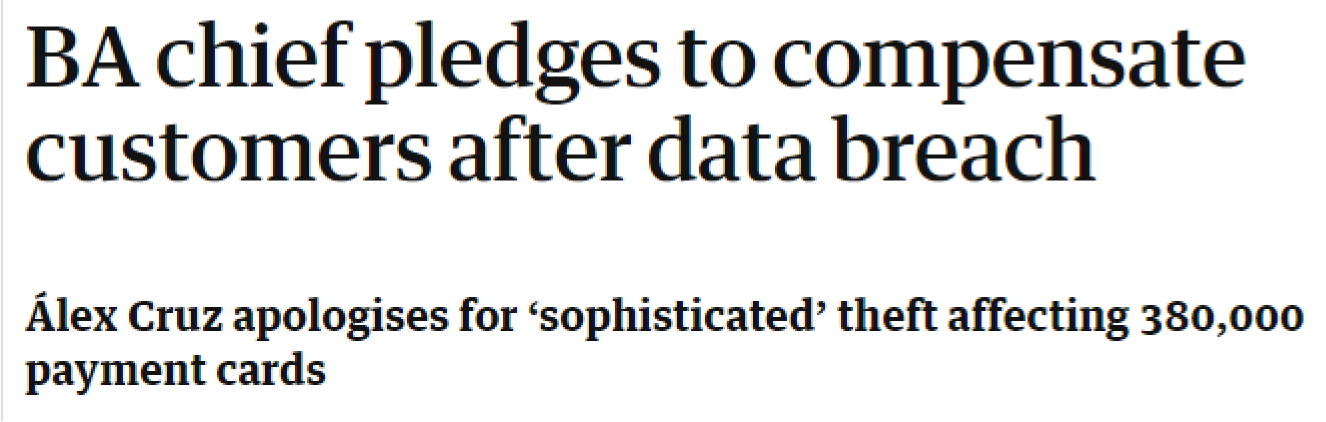
CASE STUDY: BRITISH AIRWAYS APOLOGIES



British Airways Apologises After 380,000 Customers Hit in Cyber Attack

Around 380,000 card payments were compromised with hackers obtaining names, street and email addresses, credit card numbers, expiry dates and security codes - to steal from accounts.

Reuters | **Updated:**September 7, 2018, 10:37 PM IST



BA chief pledges to compensate customers after data breach

Álex Cruz apologises for 'sophisticated' theft affecting 380,000 payment cards

https://www.theguardian.com/business/2018/sep/07/ba-british-airways-chief-alex-cruz-compensate-customers-after-data-breach
https://www.news18.com/news/world/british-airways-apologises-after-380000-customers-hit-in-cyber-attack-1871197.html

CASE STUDY: BRITISH AIRWAYS APOLOGIES

- The airline said personal and financial details of customers making or changing bookings had been compromised.

- About 380,000 transactions were affected, but the stolen data did not include travel or passport details.

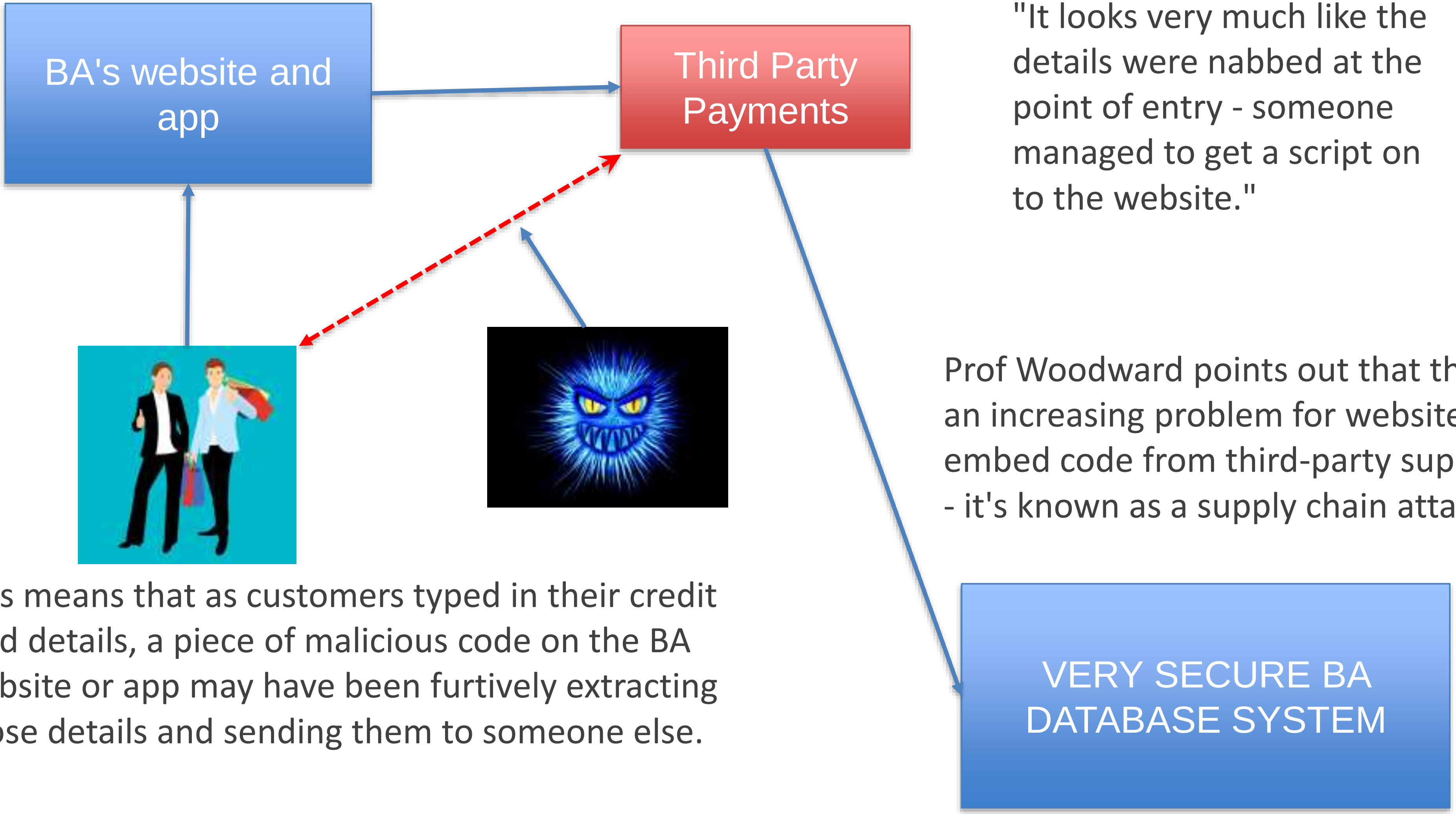
- BA said the breach took place between 22:58 BST on 21 August and 21:45 BST on 5 September. Shares in BA parent group IAG closed 1.4% lower on Friday.

- "It was name, email address, credit card information - that would be credit card number, expiration date and the three digit [CVV] code on the back of the credit card," said BA boss Mr Cruz.

- BA insists it did not store the CVV numbers. This is prohibited under international standards set out by the PCI Security Standards Council.

https://www.bbc.com/news/uk-england-london-45440850

CASE STUDY: BRITISH AIRWAYS APOLOGIES



BA's website and app

Third Party Payments

VERY SECURE BA DATABASE SYSTEM

"It looks very much like the details were nabbed at the point of entry - someone managed to get a script on to the website."

Prof Woodward points out that this is an increasing problem for websites that embed code from third-party suppliers - it's known as a supply chain attack

This means that as customers typed in their credit card details, a piece of malicious code on the BA website or app may have been furtively extracting those details and sending them to someone else.

https://www.bbc.com/news/technology-45446529

CASE STUDY: BRITISH AIRWAYS APOLOGIES

"You can put the strongest lock you like on the front door," he said, "but if the builders have left a ladder up to a window, where do you think the burglars will go?"

Prof Woodward

ISACA®
Trust in, and value from, information systems
Harare Chapter

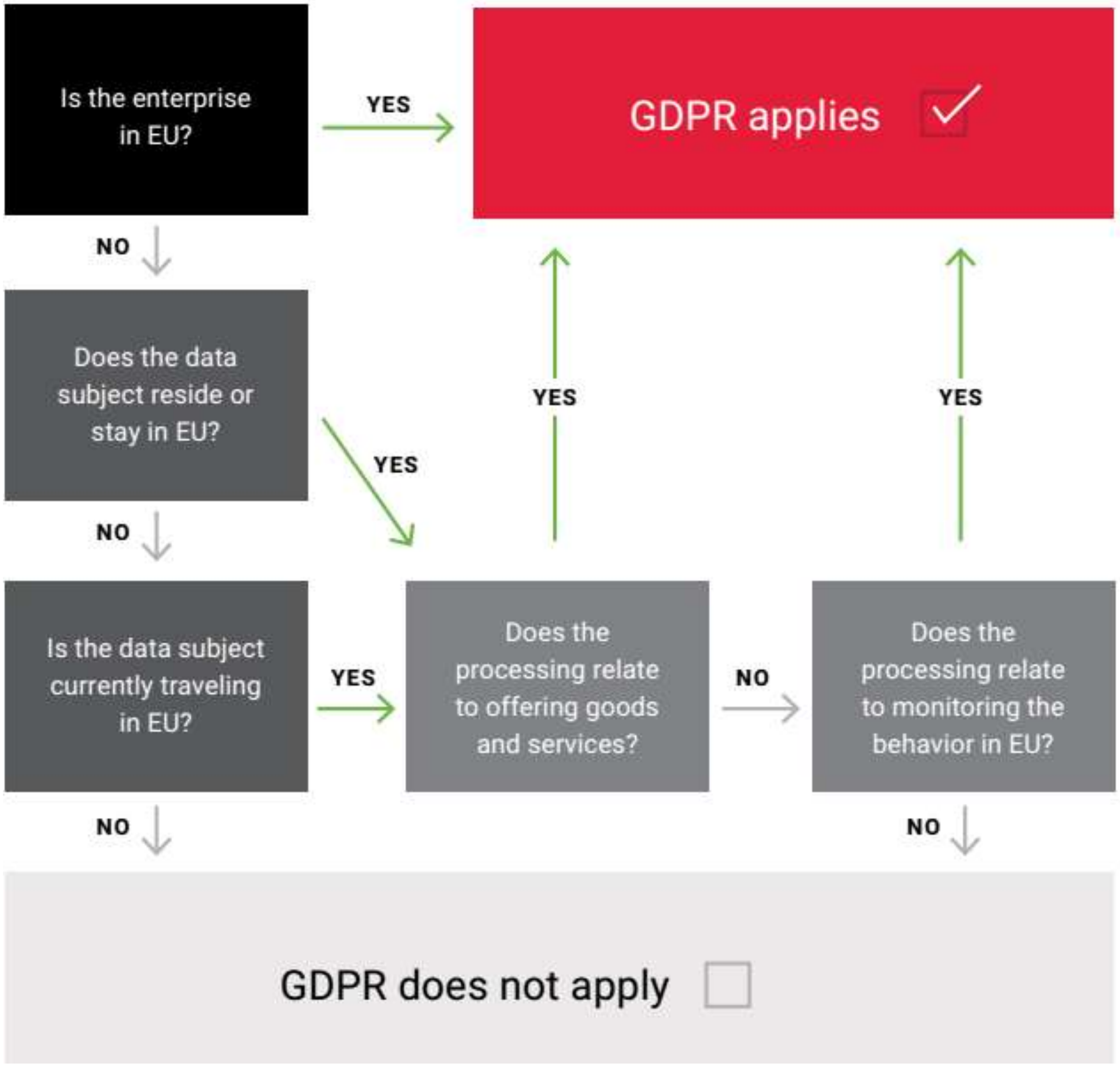
PRIVACY

ISACA®
Trust in, and value from, information systems

PRIVACY-GDPR

Under GDPR, fines can be up to 4% of annual global revenue. BA's total revenue in the year to 31 December 2017 was £12.226bn, so that could be a potential maximum of £489m.

WHY SHOULD WE KNOW IT, WE ARE NOT IN EU?



Is the enterprise in EU?

YES

GDPR applies ☑

NO

Does the data subject reside or stay in EU?

YES

YES

YES

NO

Is the data subject currently traveling in EU?

YES

Does the processing relate to offering goods and services?

NO

Does the processing relate to monitoring the behavior in EU?

NO

NO

GDPR does not apply □

urce: Varankevich, ırhei; “Territorial scope of ɛ GDPR (Flowchart),” kedIn, 17 February 2017, *ɣw.linkedin.com/pulse/territ ial-scope-gdpr-flowchart-rhei-varankevich*, adapted ˊ creative commons ɜnse at *ɔs://creativecommons.org enses/by-sa/4.0/*

THE 7 CATEGORIES OF PRIVACY

1. PRIVACY OF PERSON

2. PRIVACY OF BEHAVIOR AND ACTION

3. PRIVACY OF COMMUNICATION

4. PRIVACY OF DATA AND IMAGE (INFORMATION)

5. PRIVACY OF THOUGHTS AND FEELINGS

6. PRIVACY OF LOCATION AND SPACE

7. PRIVACY OF ASSOCIATION

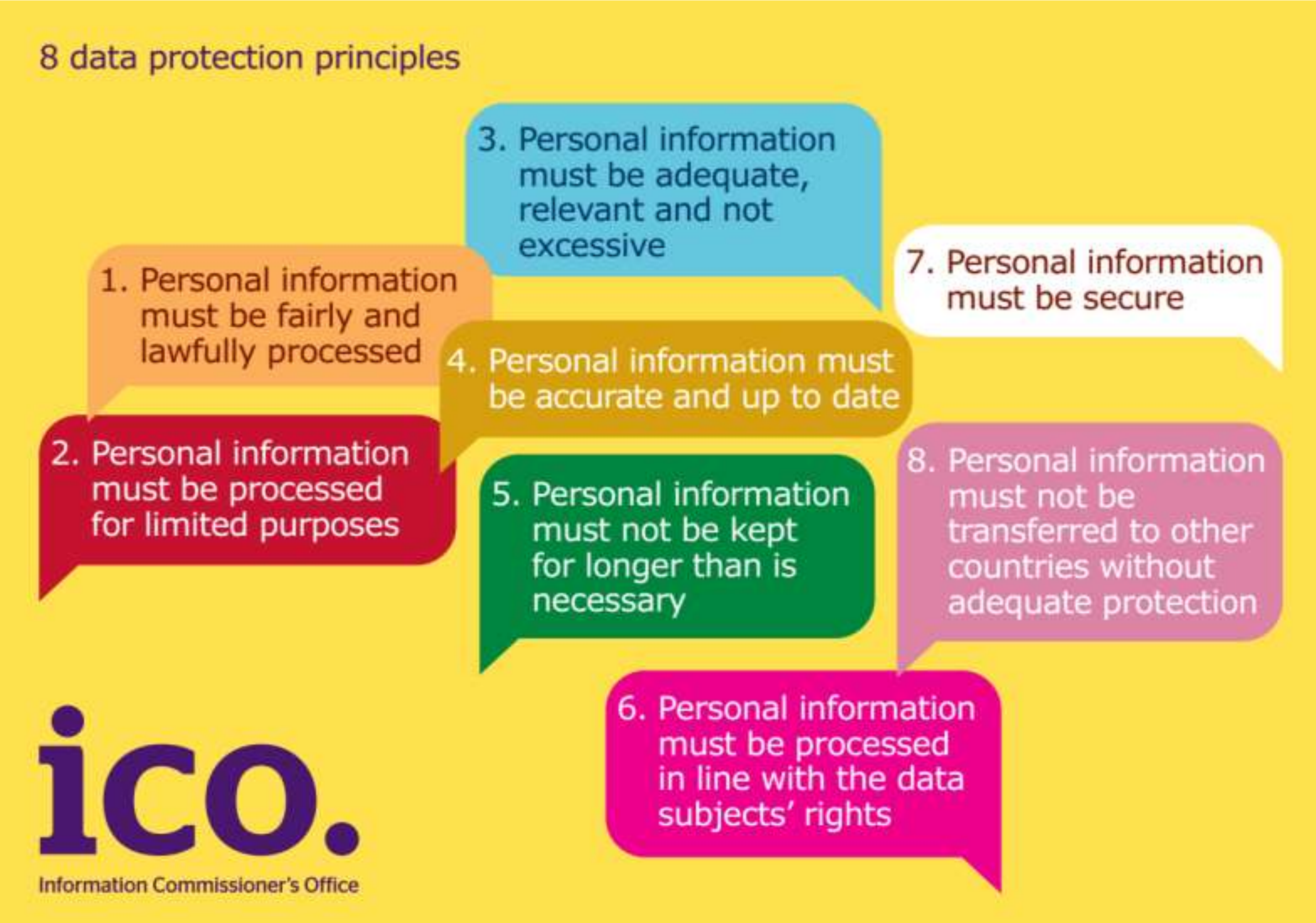
Foxit Reader PDF Document

SIX ESSENTIAL DATA PROTECTION AND PRIVACY REQUIREMENTS UNDER GDPR

1. Data security controls need to be, by default, active at all times.
2. These controls and the protection they provide must be embedded inside all applications.
3. Along with embedding the data protection controls in applications, the system must maintain data privacy across the entire processing effort for the affected data.
4. Complete data protection and privacy adds full-functional security and business requirements to any processing system in this framework for data privacy.
5. The primary requirement for protection within the GDPR framework demands the security and privacy controls implemented are proactive rather than reactive.
6. With all of these areas needed under GDPR, the most important point for organizations to understand about GDPR is transparency.

Leighton Johnson, CISA, CISM, CIFI, CISSP (@-isaca-volume-4-21-february-2018)

8 PRINCIPLES GDPR



8 data protection principles

1. Personal information must be fairly and lawfully processed
2. Personal information must be processed for limited purposes
3. Personal information must be adequate, relevant and not excessive
4. Personal information must be accurate and up to date
5. Personal information must not be kept for longer than is necessary
6. Personal information must be processed in line with the data subjects' rights
7. Personal information must be secure
8. Personal information must not be transferred to other countries without adequate protection

ico.

Information Commissioner's Office

Trust in, and value from, information systems
Harare Chapter

GOVERNANCE

Trust in, and value from, information systems

REMEMBERING GOVERNANCE

Governance—”[S]tructures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, [and] stability…

Compliance—Acting in accordance with a wish or command

Data Governance for Privacy, Confidentiality and Compliance (DGPC)-Microsoft

DGPC FRAMEWORK COMPONENTS

People-Data governance processes and tools are only as effective as the people who use and manage them.

Process- With the right people involved in the DGPC effort, the organization can focus on defining the processes involved.

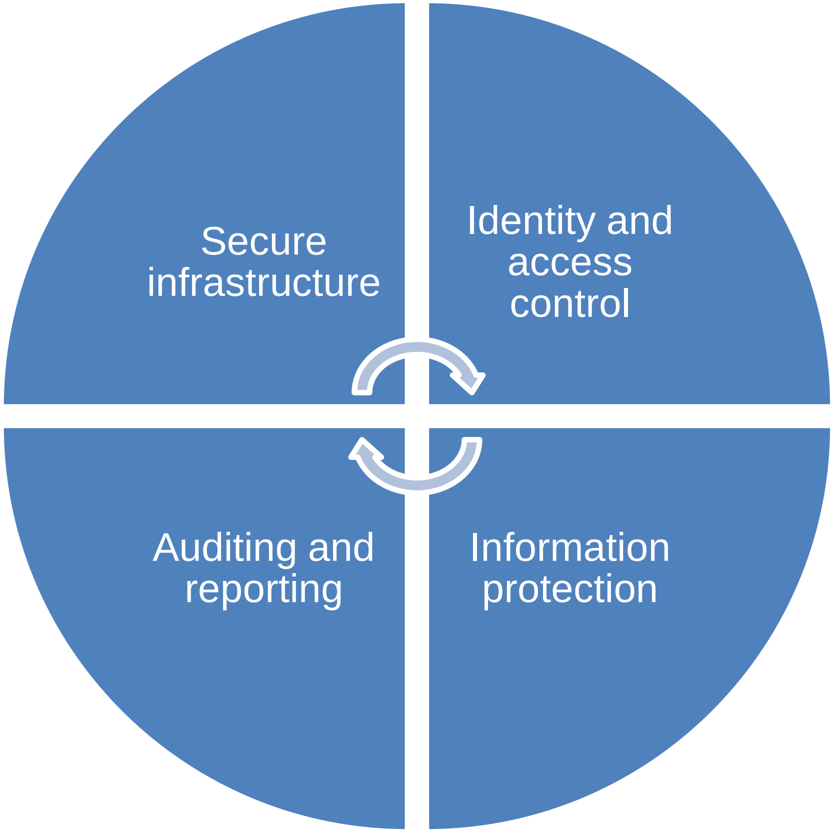
Technology- Organizations also need to systematically evaluate whether the technologies that protect their data confidentiality, integrity and availability are sufficient to reduce risk to acceptable levels

https://www.isaca.org/Journal/archives/2010/Volume-6/Pages/Data-Governance-for-Privacy-Confidentiality-and-Compliance.aspx

DGPC FRAMEWORK COMPONENTS

Technology Domains

- **Secure infrastructure**
- **Identity and access control**
- **Information protection**
- **Auditing and reporting**



DATA PRIVACY AND CONFIDENTIALITY PRINCIPLES

- **Principle 1: Honor policies throughout the confidential data life span.**

- **Principle 2: Minimize risk of unauthorized access or misuse of confidential data**

- **Principle 3: Minimize the impact of confidential data loss**

- **Principle 4: Document applicable controls and demonstrate their effectiveness.**

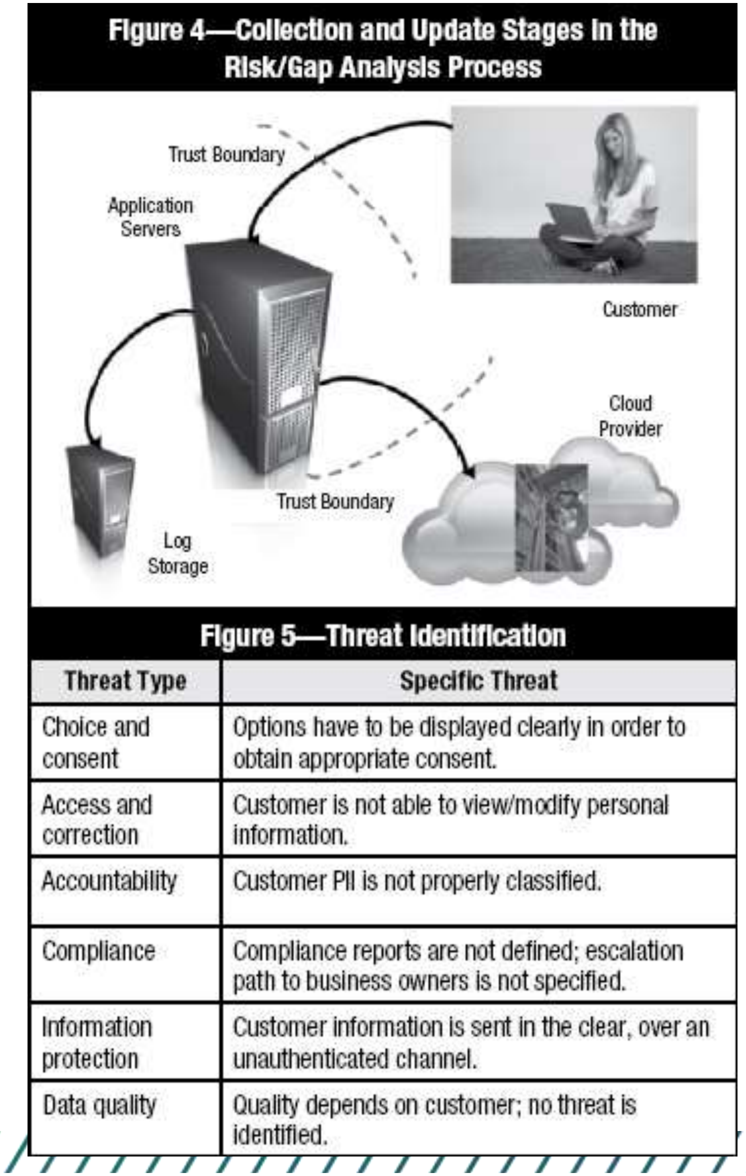


Figure 4—Collection and Update Stages in the Risk/Gap Analysis Process

Figure 5—Threat Identification

Threat Type	Specific Threat
Choice and consent	Options have to be displayed clearly in order to obtain appropriate consent.
Access and correction	Customer is not able to view/modify personal information.
Accountability	Customer PII is not properly classified.
Compliance	Compliance reports are not defined; escalation path to business owners is not specified.
Information protection	Customer information is sent in the clear, over an unauthenticated channel.
Data quality	Quality depends on customer; no threat is identified.

https://www.isaca.org/Journal/archives/2010/Volume-6/Pages/Data-Governance-for-Privacy-Confidentiality-and-Compliance.aspx

CYBERSECURITY NEXUS

Thank you

Contact: *education@isaca.org.zw, winstonz@isaca.org.zw*

Presentation by Winston Zvirikuzhe (CISA, CGEIT),

ISACA

Trust in, and value from, information systems

Harare Chapter

MY BIOGRAPHY WINSTON ZVIRIKUZHE

CURRENT-VICE PRESIDENT OF ISACA HARARE CHAPTER
PSMAS ICT AUDITOR

Qualifications

- BSc Information Systems (Hons) MSU
- Master of Business Administration (Mary Mount California University, USA)
- Certified Information Systems Auditor (CISA),
- Certified in Governance Enterprise IT(CGEIT),
- Six Sigma (Green Belt)

- Experience
- **Revenue Assurance and Risk Management**
  - Company Strategy Formulation
  - Performance Management Assurance
  - Revenue Assurance
  - Risk Assessment
  - Company Policies and Procedures reviews
- **IT – Information Technology / IS – Information Systems Advisory Services**
  - Consulting, Business Strategy & IT Strategy, Business Process Analysis
  - Project Direction & Management OR Unit Direction & Management
  - Outsourcing & Supplier Selection / Management
  - Corporate Governance

- **IT Audit Services**
  - Financials Statement Audits for IT Audit support
  - Forensic Data Analysis (ACL and IDEA Data analysis tools)
  - Internal Audit of Telecommunication Data
  - Script Development (SQL)

Positions Held in Professional Career

- ICT Auditor
- Assurance Executive (Risk and Revenue Assurance)
- Audit and Consultancy Supervisor
- Project Manager
- Client Portfolio Management
- Senior Systems Analyst

REFERENCES

a) Mark Thomas and Peter Tessin (2017)Implementing the NIST Cybersecurity Framework Using COBIT 5 A Step-by-Step Guide for Your Enterprise

b) Framework for Improving Critical Infrastructure Cybersecurity Version 1.0 National Institute of Standards and Technology February 12, 2014

c) Ed Moyle (2017) State of Cyber Security 2017 Part 2: Current Trends in the Threat Landscape

d) Alexander Klimburg (Ed.), National Cyber Security Framework Manual, NATO CCD COE Publication

e) Greg Witte and Tom Conkle (2014) Implementing the NIST Cybersecurity Framework ISBN 978-1-60420-358-5

f) https://cybersecurity.isaca.org

g) Deepak Rout (2015). Developing a Common Understanding of Cybersecurity https://www.isaca.org/Journal/archives/2015/volume-6/Pages/developing-a-common-understanding-of-cybersecurity.aspx

h) Steve Morgan, (2017, June 15)Top 5 cybersecurity facts, figures and statistics for 2017 Retrieved from http://www.csoonline.com/article/3153707/security/top-5-cybersecurity-facts-figures-and-statistics-for-2017.html

i) ITnewsAfrica (2017, March 7) 10 Biggest Cyber Crimes and Data Breaches. Retrieved from http://www.itnewsafrica.com/2017/03/10-biggest-cyber-crimes-and-data-breaches/

j) Limor Kessem (2016, December 20)Year in Review: Top Three Cybercrime Threats of 2016. Retrieved from https://securityintelligence.com/year-in-review-top-three-cybercrime-threats-of-2016/

k) Pictures from https://pixabay.com/

l) Isaca.org (2015, December 16)ISACA Identifies Five Cyber Risk Trends for 2016. Retrieved from http://www.isaca.org/About-ISACA/Press-room/News-Releases/2015/Pages/ISACA-Identifies-Five-Cyber-Risk-Trends-for-2016.aspx

m) https://www.scmagazine.com/awards/