DATA BREACHES: HOPE FOR THE BEST, PLAN FOR THE WORST

We need a new breed of compliance officer

06 SEP 2019

Project: **CISA CONFERENCE**
Client: **COMPLIANCE INSTITUTE**
Prepared by: **ELIZABETH DE STADLER**

novation consulting

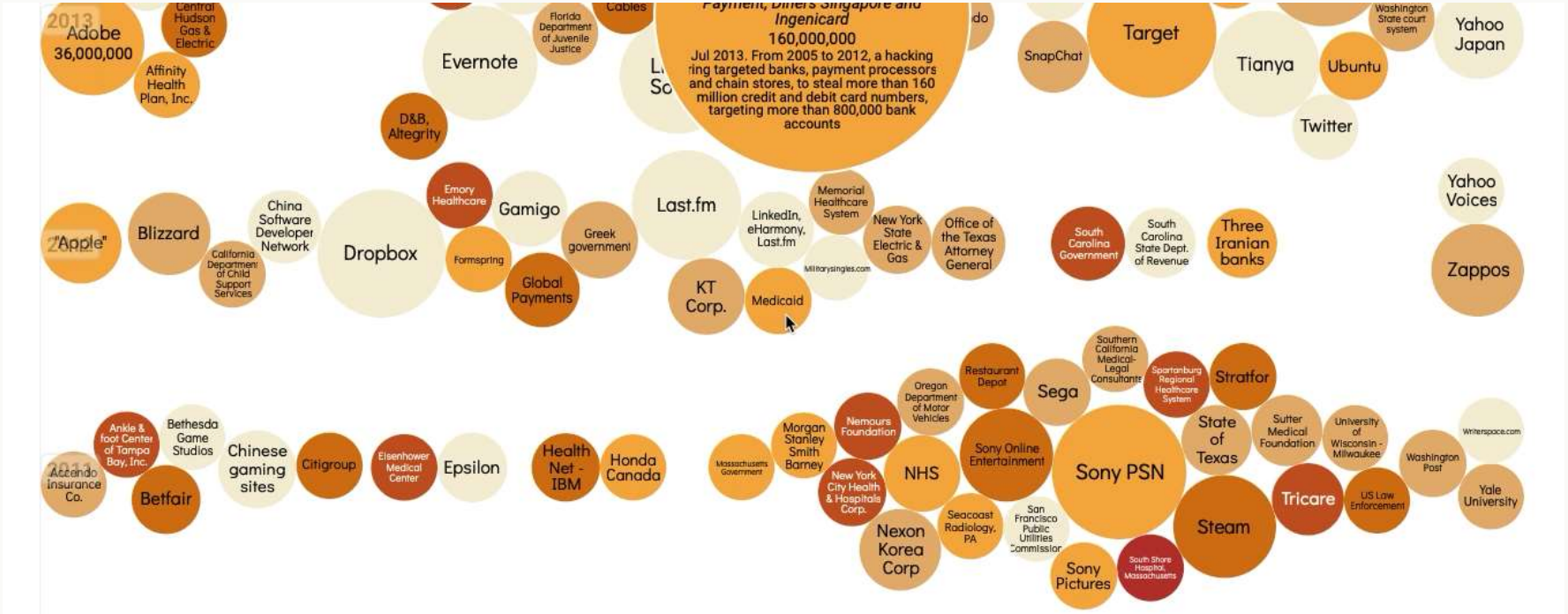
A NEW DAY
A NEW BREACH

(LET'S LOOK AT SOME NUMBERS)

“There are only two types of companies, those that know that they’ve been compromised, and those that don’t know.”

- Dmitri Alperovitch, McAfee VP of Threat Research

SPOT THE TREND



JUST IN THE LAST YEAR

THE COST OF A DATA BREACH

There are four cost centres:

- Detection and escalation
- Post data breach response
- Notification
- Lost business

WHAT SHOULD COMPLIANCE BE DOING?

(LESSONS AND NEW SKILLS)

#1 SOLVE THE PR PROBLEM

(WHY DON'T THEY LIKE US)

#Complianoscopy

> “Compliance is like a colonoscopy: People may need it, but they don’t want it, they don’t like it and they certainly don’t want to talk about it. (And they absolutely don’t want any more than is necessary).”

- Sean Graham, Five reasons Compliance is “meh”

#2 THIS IS NOT AN IT PROBLEM

(IT IS A PEOPLE PROBLEM)

> “The security problems we're now facing can't be fixed with products alone. We can't fix them with more security analysts any more than a retailer could fix shoplifting by assigning a security guard to watch every shopper as they wander around the store.”

- Adrian Sanabria, One of the good hackers, Security analyst

#3 AIM FOR CONSCIOUS INCOMPETENCE

(KNOW ENOUGH SO YOU CAN COLLABORATE)

> One of the main cyber-risks is to think they don't exist. The other is to try and treat all potential risks. Fix the basics, protect first what matters for your business and be ready to react properly to pertinent threats. Think data, but also business services integrity, awareness, customer experience, compliance, and reputation.

- Stephane Nappo, Global Chief Information Security Officer, 2018 Global CISO of the year

HAVE A WORKING UNDERSTANDING OF:

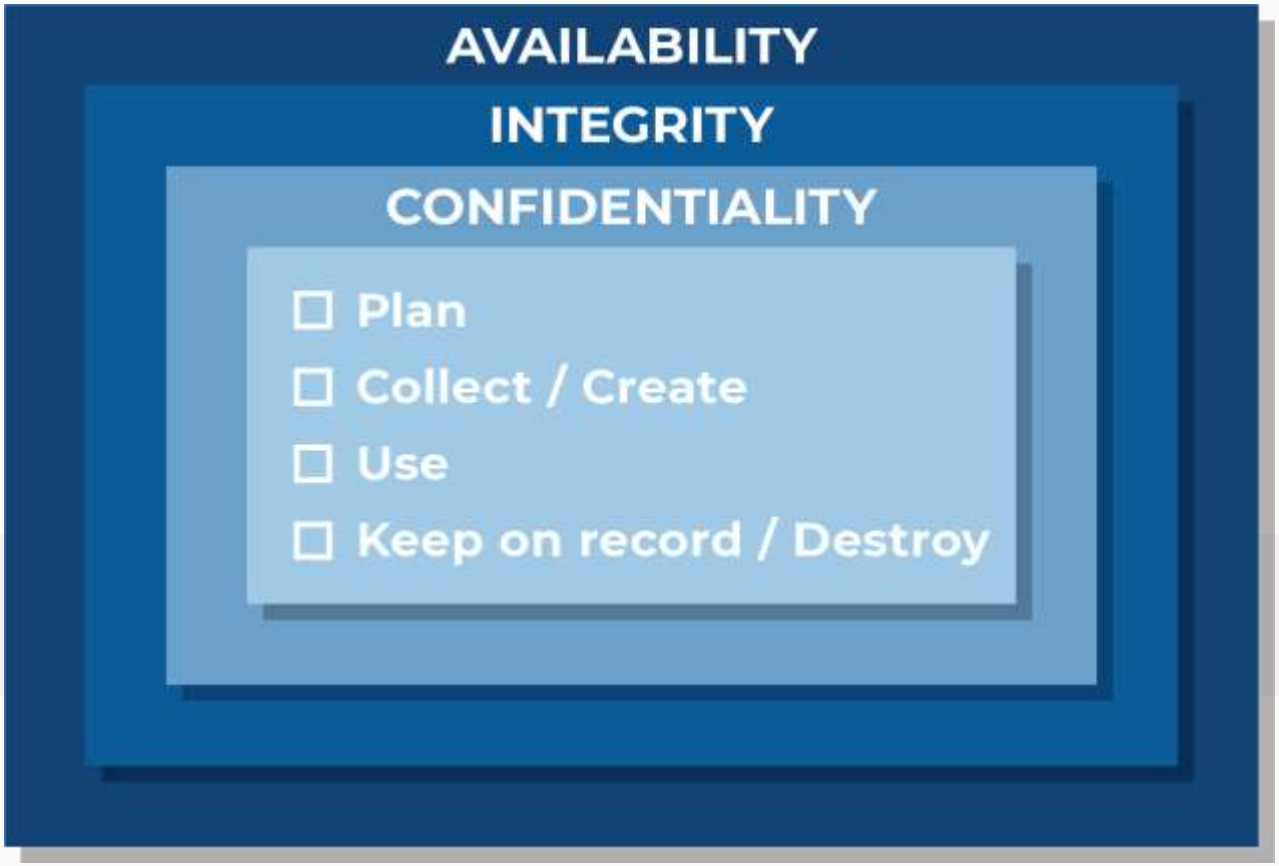
- **Risk management:** Managing uncertainty and making educated decisions.
- **Information Security Management and Data Governance:** That *&^%$# that IT does.
- **Business Continuity Management:** What is the plan when the *&^$#!& hits the fan.


JASON
STATHAM
LI
BINGBING
RAINN
WILSON
RUBY
ROSE
THE
MEG

SWIMMING IS DANGEROUS

- **Avoid:** Stop swimming.
- **Reduce:** Buy a bigger boat.
- **Transfer:** Outsource the swimming (to Jason Statham).
- **Accept:** Swim anyway.
- **Share:** Get life insurance.

HERE IS THE LIFE CYCLE



WHAT IS THE CIA TRIAD?

- **Confidentiality:** Access should be granted on a ‘need to know’ basis. Also known as ‘roles-based’ access which should be coupled with the ‘least privilege’ principle.
- **Integrity:** Ensure that information isn’t tampered with. Changes to information should be controlled.
- **Availability:** Ensure that the services of the company are available through Business Continuity Management.

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.

Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

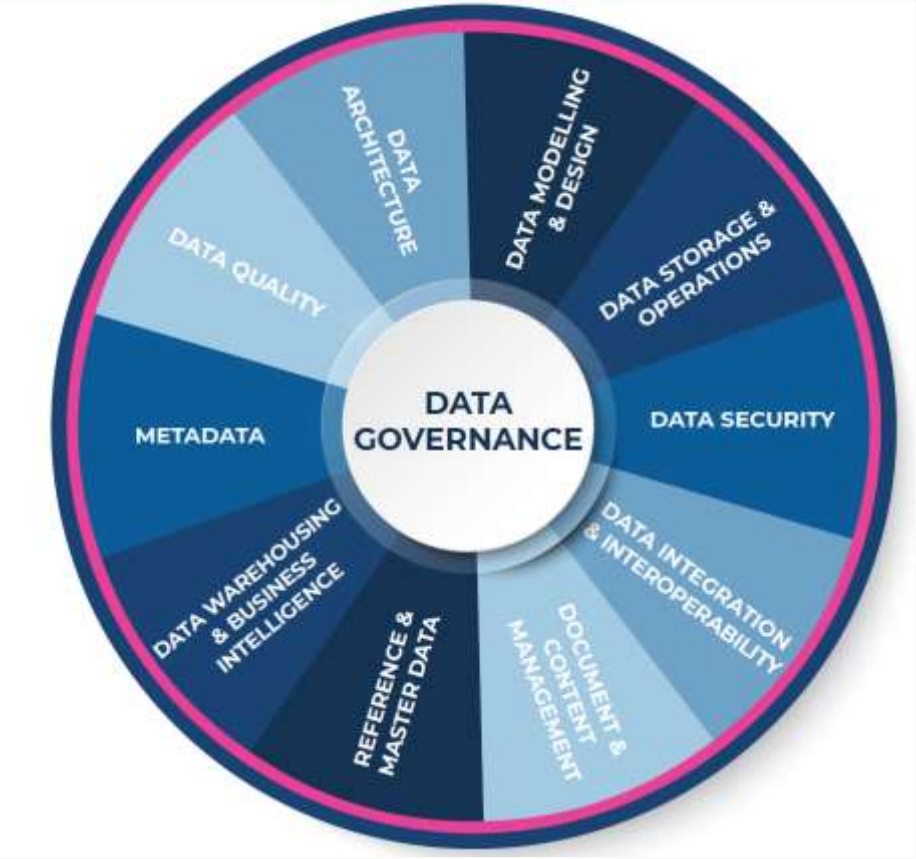
Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

WHAT IS DATA GOVERNANCE?

…an overarching strategy for organisations to ensure the data they use is clean, accurate, usable, and secure




OUR DISASTER RECOVERY PLAN GOES SOMETHING LIKE THIS...
www.dilbert.com scottadams@aol.com
HELP! HELP!
© 2000 United Feature Syndicate, Inc.
8/15/00
SOMEDAY WE HOPE TO HAVE A BUDGET.

#4 NO POLICY IS BETTER THAN AN UNIMPLEMENTED POLICY

(STOP TICKING BOXES)

HOW DO YOU IMPLEMENT?

- **Impact on other policies and procedures:** Do we need new ways of working?
- **Impact on infrastructure and equipment:** Do we need new buildings, equipment, hardware, software or menswear?
- **Impact on people:** Do we need new people, do the existing people need new KPIs or do they have the skills to do what we are asking of them?

#5 LEARN MORE ABOUT PEOPLE

(WHY 'OH BEHAVE' DOESN'T WORK)

> “The methods that will most effectively minimize the ability of intruders to compromise security are comprehensive user training and education. Enacting policies and procedures simply won’t suffice.”

- Kevin Mitnick, convicted hacker

THE SCIENCE OF BEHAVIOUR

Why they won't follow our policies:

- **The psychology of fear:** Understand the threat.
- **Social engineering and hot states:** We get phished when we are in a hot state (greed, panic, desire) and can't be rational.
- **Similarity or simulation heuristic:** We underestimate cyber threats, because it hasn't happened to us before or we can't imagine it.
- **Fluency heuristic:** What the hell is 'two-factor authentication'.

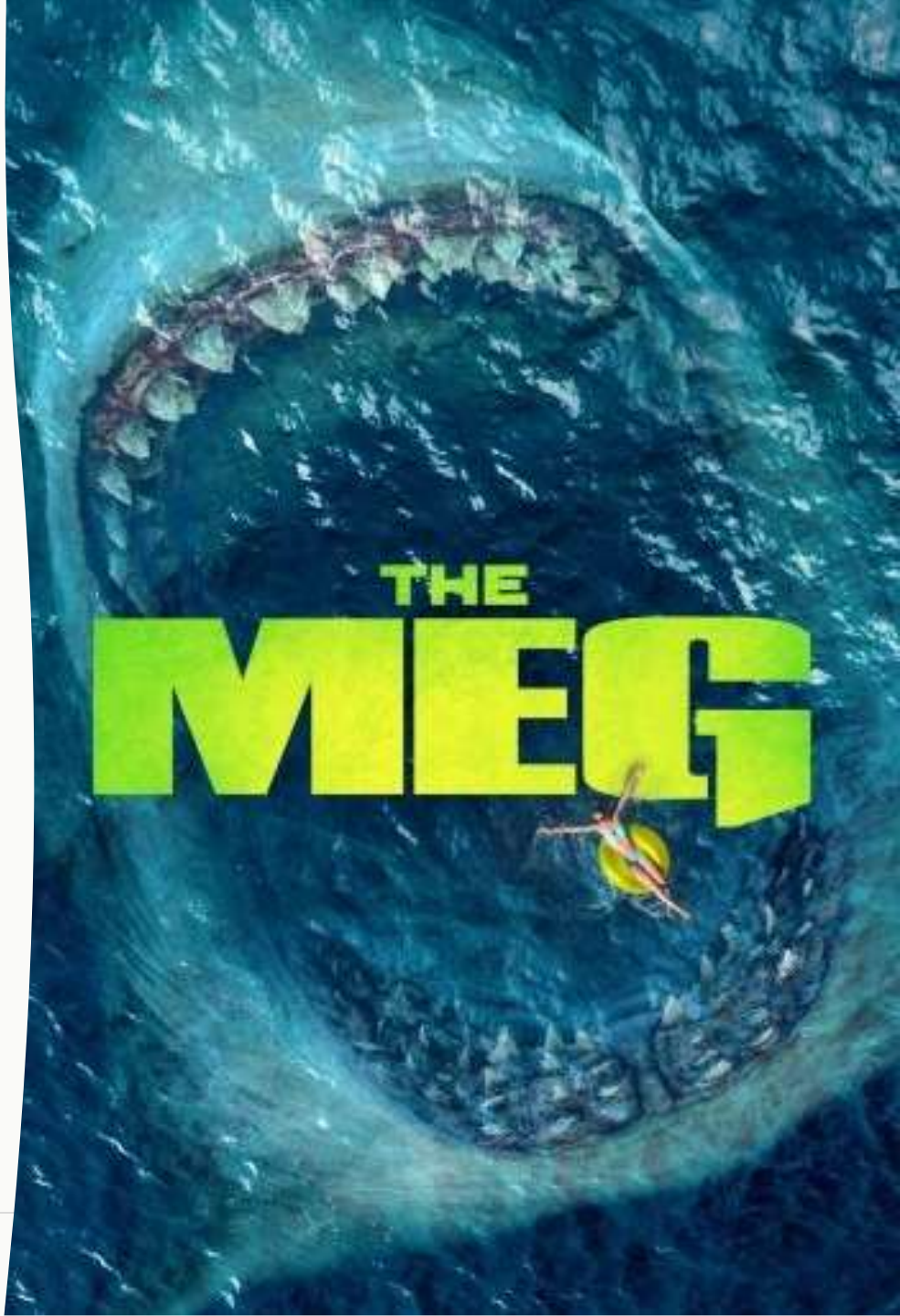
#6 HOPE FOR THE BEST

(PLAN FOR THE WORST AND SAVE $1.2 MILLION)

PLAN FOR THE WORST

This is what you need:

- an incident response **policy and procedure**
- a **incident response team** (including external Infosec specialists, forensic auditors etc)
- **disaster recovery** plans (cyber resilience and fault tolerant systems and processes)
- **disaster communications** specialists on hand (this is a specialist field – many marketers suck at it)
- an **attorney** to help you with your notification to the Regulator and to preserve evidence (privilege must attach)
- **test** your procedure and IRT and then test again
- **Train (nudge)** your employees **and then train them again**



THANK YOU!

elizabeth@novcon.co.za