HIVE LOGIC

GDPR AND SECURITY

Presentation delivered by;

Mr. Simon Moore

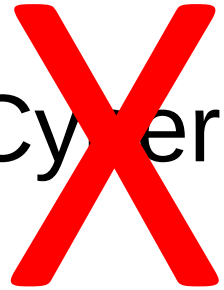
30th May 2018

BRAZILIAN CHAMBER OF COMMERCE IN GREAT BRITAIN

Compliant

To be GDPR compliant

You need to be Cyber Secure



So lets look at what that means

HIVE LOGIC

Cyber Security

Sufficient

Simple

Affordable

Understandable

Sufficient

The security in place should address the risks in your business.

Simple.

If it doesn't, it is not sufficient.

Stack rank the risks and work your way down.

When you run of budget, if your next unmet risk is too high, get more budget.

HIVE LOGIC

Cyber Security

Simple

Complexity costs.

Complex attracts short cuts

The real costs are in the operations, the breaches,

Cost of change often stops things happening, yet now some of the solutions available are fundamentally simple.

Pure cloud, straight to cloud,
Or software defined.

HIVE LOGIC

Cyber Security

There is no new money

Security doesn't increase profits!

Security is not a positive experience
Everything is negative – ruined reputations, fines, rectification costs.

East to say it costs more than doing it right.

Affordable

$171 million Sony estimated for the breach of its Playstation Network in 2011

Then, second corporate hit in 2015

former federal cyber crimes prosecutor, estimated costs could run up to $70 million.

HIVE LOGIC

Cyber Security

The biggest single source of security breaches, is from people

We have to help our staff not make mistakes.

Make the security policy understandable so people can follow it

1 click mistakes have to be removed!

Understandable

- **Better way:**
  - Make security an enabler for digital transformation!

HIVE LOGIC

I can't

Cloud Applications

Mobile Applications

Block-Chain

Mobility

Internet of Things – automated cloud accessed "stuff"

I can't innovate!

it increases Cyber risk

☹

Increased presence on the web

Foreign Markets

Extend applications into the supply chain

Store and Analyse customer Data

HIVE LOGIC

The Answer?

There is no new money, and dealing with risk, is a tomorrow problem.

Cyber Security – might not happen to me. Dealing with the risk, will cost me money now, money I don't have, or I need elsewhere. AND….

HIVE LOGIC

The Real Answer – challenge the assumption

Design to introduce security that improves the state of my business:

- It makes new money
- It helps reduce costs

HIVE LOGIC

I can

I can be more mobile

I can extend applications into the supply chain

I can use mobile applications

I can Store and Analyse customer Data *(appropriately ☺)*

I am secured!

Time to Innovate ☺

I can invest in Foreign Markets

I can have an increased presence on the web

I can use IOT and increase automation

I can embrace Cloud Applications

I can use Blockchain and new ways of moving money

HIVE LOGIC

The MAGIC answer

Create positive cash through innovation

As part of the project cost - include Security

The Security introduced allows more innovation projects

HIVE LOGIC

A case Study

Carphone Warehouse

Part of the Dixons Group

PC World etc….

HIVE LOGIC

There, but for the grace of god (bftGoG)

- Car Phone Warehouse ICO fine. The same people who are going to apply the GDPR fines!
- The default security policy not updated or followed

Affordable

Adding security does not help the top line, and it adds cost to a business without improving profitability or productivity. So it is not surprising that most companies (in my opinion) would find themselves carrying some of the risks, that resulted in this fine.

- CW paid more for their defence than they were fined!

  £400K

- CW claimed that the ICO imposed unjustifiable high standards for security - this was rejected. Apparently being as bad as everyone else is not a mitigation.

Understandable

- The ICO held the view that just having the vulnerabilities was causal to the attack. This is like leaving a home window open inviting a burglary.

HIVE LOGIC

Simple

- **Deficient patching.**
  - Patching is the top of every security advisory list

- The worries most business have is that installing the patches does not often fit in with plans for downtime, also they worry that the patch will cause disruption. So ICT teams try to be efficient on how and when patches are incorporated. In my experience, there is often internal conflict between ICT infrastructure managers on a tight operational budget, and ICT security teams pushing for fast patching. This conflict is in every company and needs to be addressed. Being years out of date

HIVE LOGIC

Simple

- CW had policies in place that were not followed or reviewed.

HIVE LOGIC

Sufficient

- The ICO held the view that an Identity and Access Management (IDAM) system should have been in place.
- As to how the attacker got those credentials? – was not asked
- Your cyber maturity is shown by your weakest element, not your strongest!

Sufficient

- **No Web Application Firewall (WAF).** Pretty straight forward one. If you have a website, protect it. Equally, and not in this breach, if you have a cloud - protect it!

- **No Vulnerability Scanning.** The attacker scanned the network using standard software, and found the open window. From this report one can assert that the ICO sees pen-testing etc, as a fundamental component of any security system.

Sufficient

- **Anti Virus.**

- the ICO found that whilst AV wouldn't have stopped this attack (probably as the attacker had valid credentials) they still found against CW on the basis that their infrastructure (attack not withstanding) was in breach of the requirements. ie; even if they hadn't been attacked they could have been fined anyway.

HIVE LOGIC

Simple Steps

- **One step taken by the Government to make things simple was to introduce and support**
- **Cyber Essentials.**
- **And this was covered in a previous**
- **workshop.**

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**

HIVE LOGIC

Cyber Security

Sufficient

Simple

Affordable

Understandable

Risks Managed

Reduce complexity

Release capital, merge with Digital Transformation projects

Staff Awareness and training