aql®

RIPE IoT Roundtable Meeting 21 September 2017

CSP Yorkshire & Humber

In partnership with aql

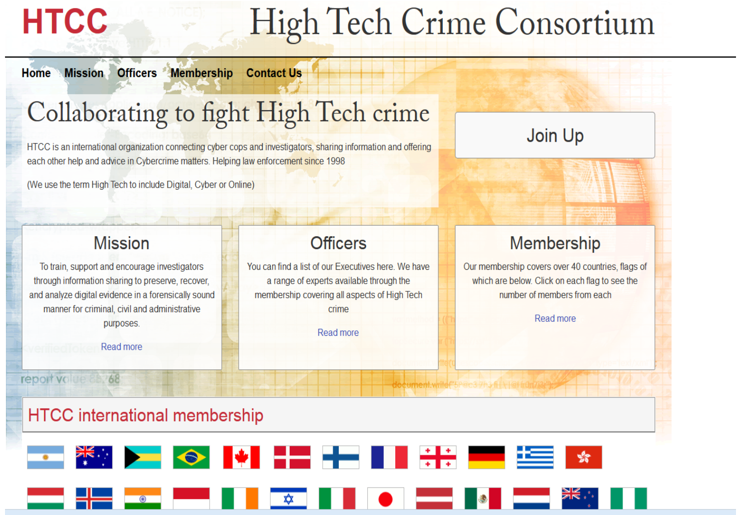
Stuart Hyde QPM

ilkleybusinessforum
promoting business in the LS29 area

EUROPOL

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

CEOP
A National Crime Agency command



HTCC High Tech Crime Consortium

Home Mission Officers Membership Contact Us

Collaborating to fight High Tech crime

HTCC is an international organization connecting cyber cops and investigators, sharing information and offering each other help and advice in Cybercrime matters. Helping law enforcement since 1998

(We use the term High Tech to include Digital, Cyber or Online)

Join Up

Mission

To train, support and encourage investigators through information sharing to preserve, recover, and analyze digital evidence in a forensically sound manner for criminal, civil and administrative purposes.

Read more

Officers

You can find a list of our Executives here. We have a range of experts available through the membership covering all aspects of High Tech crime

Read more

Membership

Our membership covers over 40 countries, flags of which are below. Click on each flag to see the number of members from each

Read more

HTCC international membership

CSP
A CATALYST FOR COLLABORATION

348 Million identities exposed (out of 7.5Bn)

594 Million affected by cyber crime

1 in 3 don’t have a password on their phone

Your world

In partnership with aql

Symantec

Kaspersky

Trend Micro

IOCTA

A CATALYST FOR COLLABORATION

Symantec & Kaspersky

- Subversion and sabotage
- Ransomware escalating
- New frontiers: IoT and cloud
- Resurgence of email as attack channel
- Phishing increase
- Android banking malware

Trend Micro

- **Ransomware** deeper, and wider non-desktop targets.
- **Business Email Compromise** attacks
- More Adobe and **Apple vulnerabilities**
- **Smart devices** denial-of-service Attacks and **Internet of Things**
- The **General Data Protection Regulation** (GDPR) implementation looms nearer

IOCTA

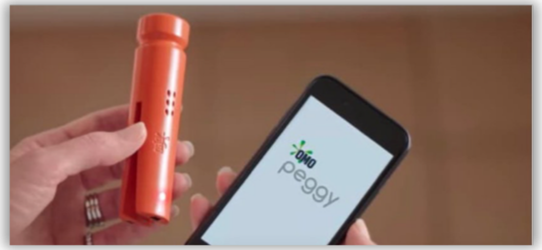
- Encrypting ransomware
- Malware on mobile devices
- Darknet forums
- CEO fraud
- Contactless cards
- DDoS attacks
- Data remains a key commodity for cybercriminals

aql

Some examples of *everything*…

CISP Yorkshire & Humber

In partnership with aql



CISP
A CATALYST FOR COLLABORATION

Vulnerabilities

Thing/RFID

WiFi/Bluetooth

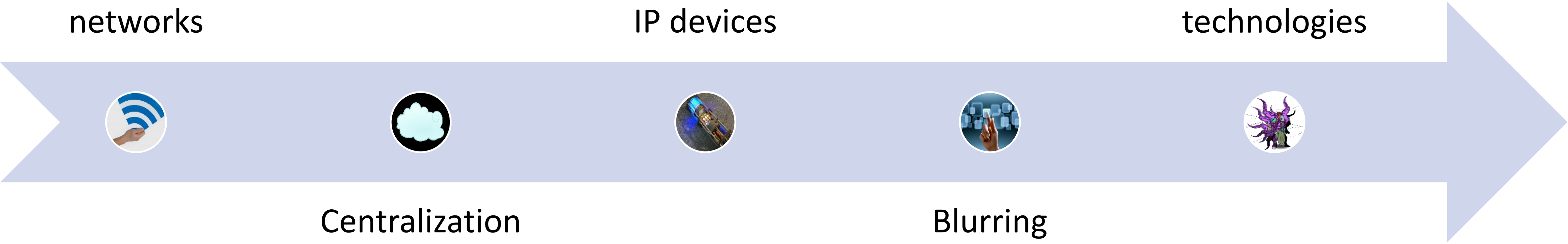
Cloud

PICNIC

Problem
Is in the
Chair
Not
In the
Computer

In partnership with aql

A CATALYST FOR COLLABORATION



Increase in broadband and wireless networks

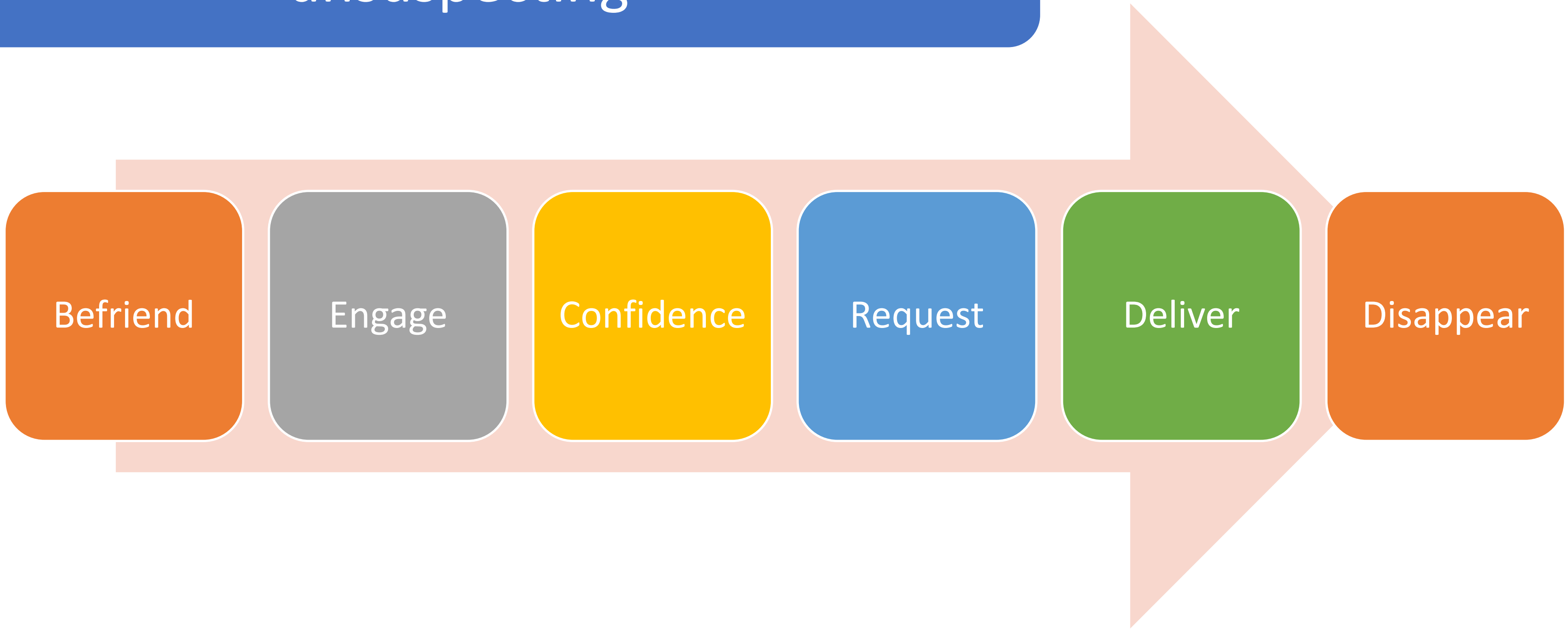
Centralization and widespread cloud computing

Proliferation of IP devices

Blurring work/personal 'Bring Your Own' approach to enterprise IT

Emergence of potentially disruptive technologies

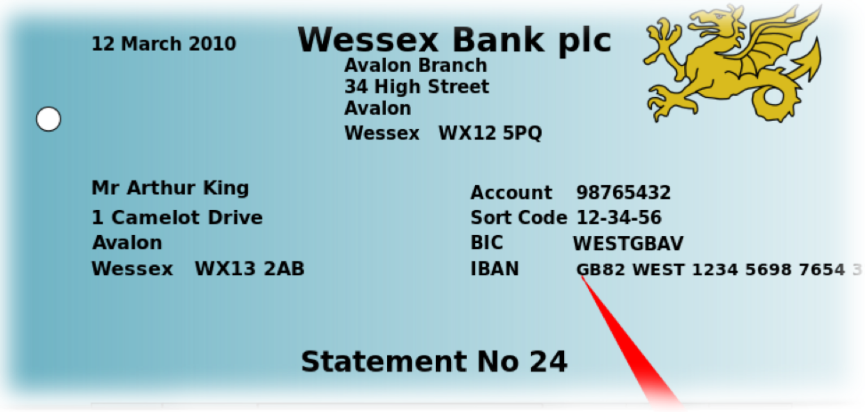
Using Social Media for grooming the unsuspecting



GET SAFE ONLINE .org™

Password
seecateek

National Cyber Security Centre
a part of GCHQ



12 March 2010

Wessex Bank plc
Avalon Branch
34 High Street
Avalon
Wessex WX12 5PQ

Mr Arthur King
1 Camelot Drive
Avalon
Wessex WX13 2AB

Account 98765432
Sort Code 12-34-56
BIC WESTGBAV
IBAN GB82 WEST 1234 5698 7654

Statement No 24

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

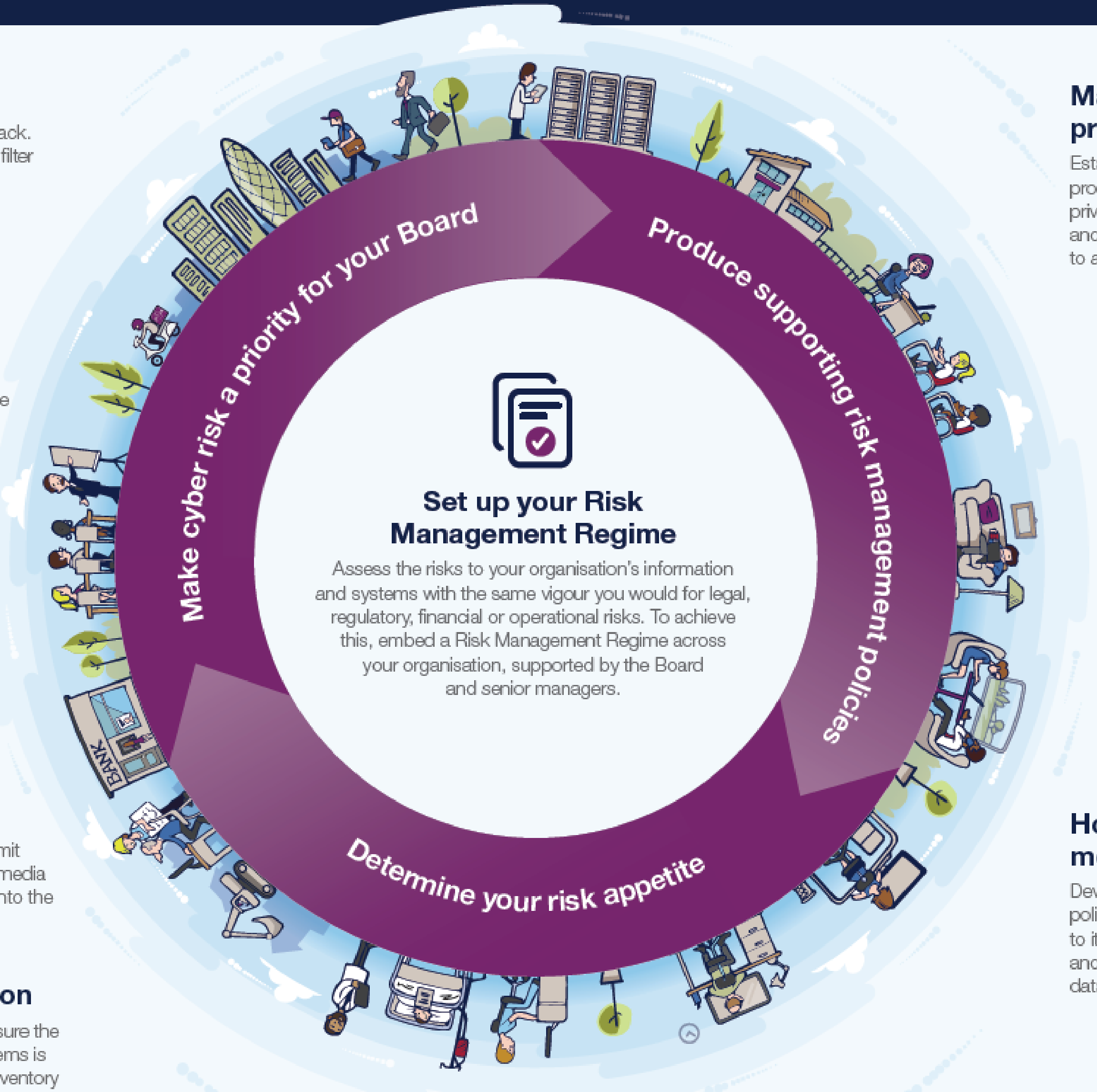
Produce relevant policies and establish anti-malware defences across your organisation.

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.


Make cyber risk a priority for your Board
Produce supporting risk management policies
Determine your risk appetite
BANK

Set up your Risk Management Regime

Assess the risks to your organisation's information and systems with the same vigour you would for legal, regulatory, financial or operational risks. To achieve this, embed a Risk Management Regime across your organisation, supported by the Board and senior managers.

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.

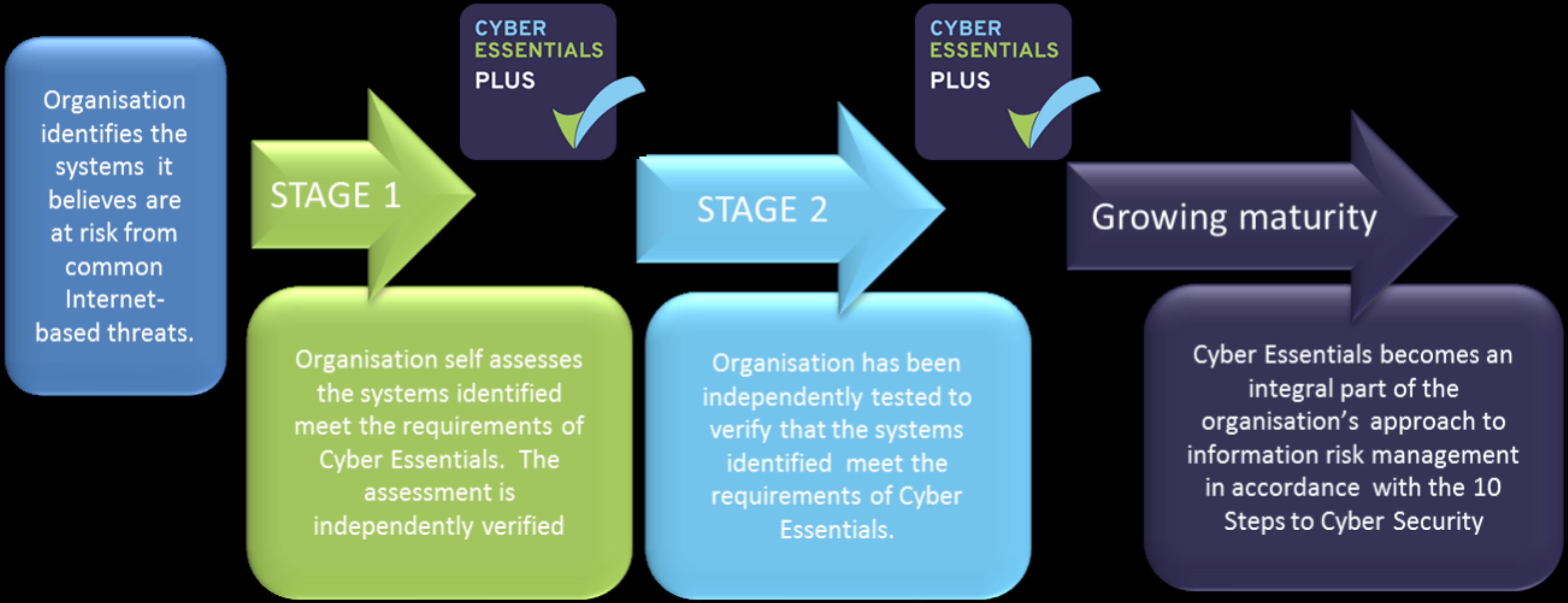
Monitoring

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



Organisation identifies the systems it believes are at risk from common Internet-based threats.

STAGE 1

Organisation self assesses the systems identified meet the requirements of Cyber Essentials. The assessment is independently verified

STAGE 2

Organisation has been independently tested to verify that the systems identified meet the requirements of Cyber Essentials.

Growing maturity

Cyber Essentials becomes an integral part of the organisation's approach to information risk management in accordance with the 10 Steps to Cyber Security

aql

ISO 27001

CSP Yorkshire & Humber

In partnership with aql

- Organisations of any type, size or nature
- Information Security Management System
- Leadership
- Planning – identify & analyse
- Support - competent resources
- Operation - assessing and treating information risks
- Performance evaluation - monitor, measure, analyze
- Improvement - address audits and reviews

CSP

A CATALYST FOR COLLABORATION

aql

General Data Protection Regulation (GDPR)

CSP Yorkshire & Humber

In partnership with aql

- All data
- May 2018
- Will be part of your working lives
- Brexit won’t change it
- 4% fine
- Data is the new oil

CSP
A CATALYST FOR COLLABORATION

CSP

CiSP
Yorkshire & Humber

In partnership with aql

Cyber-security Information Sharing Partnership

CiSP

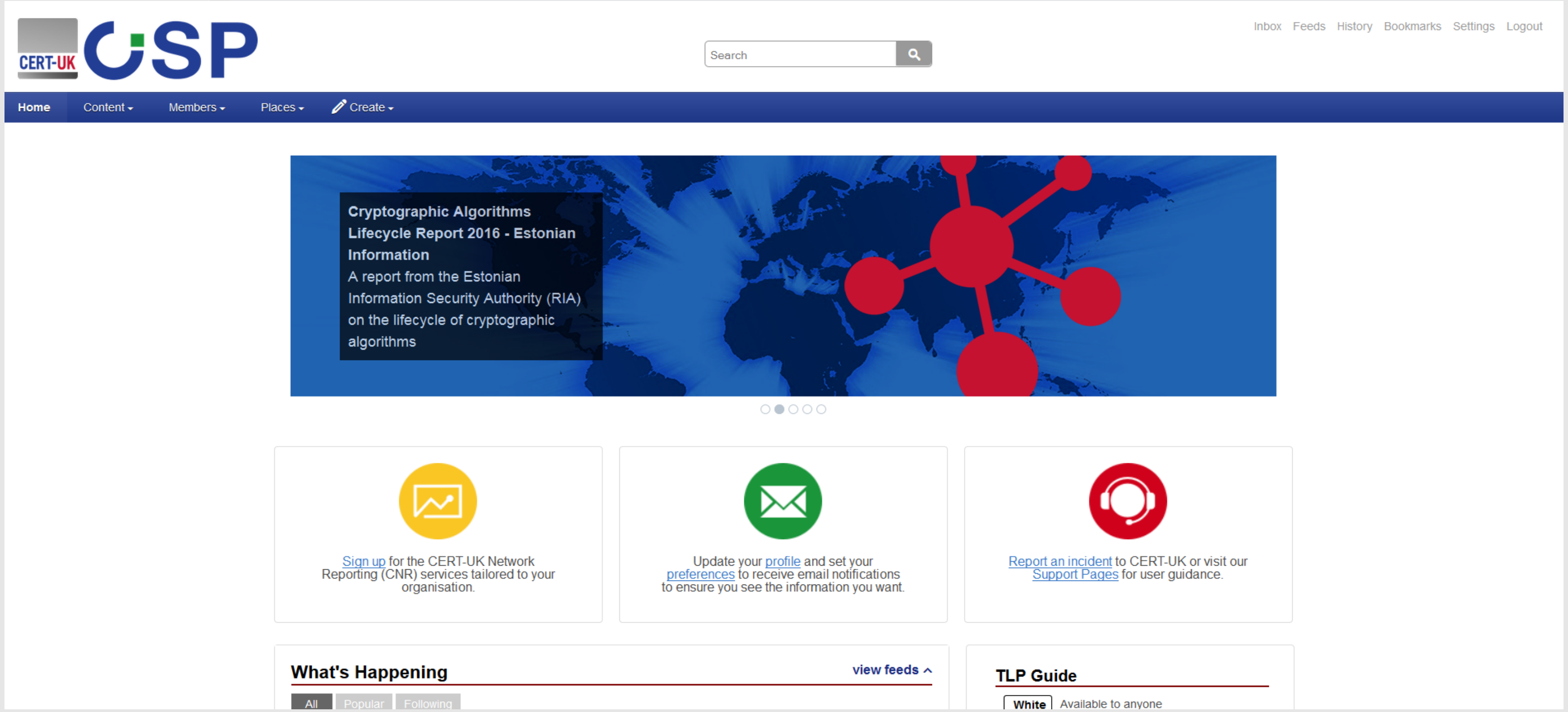
A CATALYST FOR COLLABORATION

FREE

CSP

CSP Yorkshire & Humber

In partnership with aql



Cryptographic Algorithms Lifecycle Report 2016 - Estonian Information
A report from the Estonian Information Security Authority (RIA) on the lifecycle of cryptographic algorithms

Sign up for the CERT-UK Network Reporting (CNR) services tailored to your organisation.

Update your profile and set your preferences to receive email notifications to ensure you see the information you want.

Report an incident to CERT-UK or visit our Support Pages for user guidance.

What's Happening

TLP Guide

White Available to anyone

@YHCisp

A CATALYST FOR COLLABORATION

aql®

CiSP Yorkshire & Humber

In partnership with aql

Stuart Hyde QPM

@stuarthydeqpm
@YHcisp

stu@stuhyde.com
www.ncsc.gov.uk/cisp

CiSP
A CATALYST FOR COLLABORATION