SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Wiltshire Council

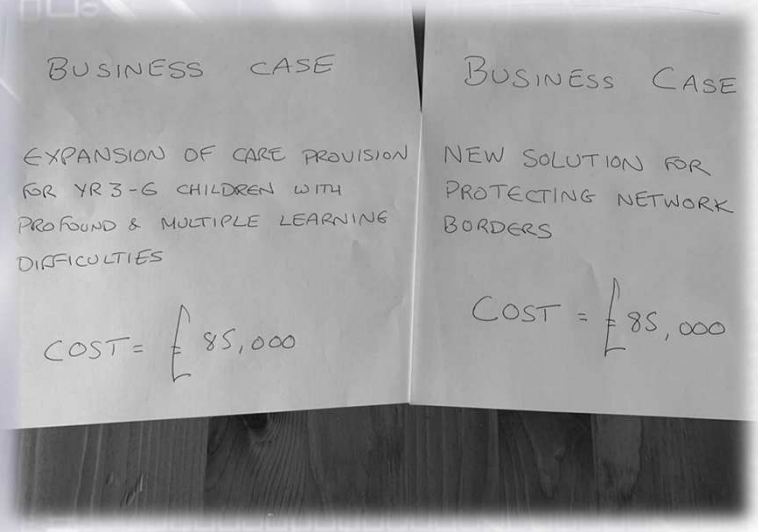
Cyber Is For Everyone

Why Cyber Security at Wiltshire Council is everyone's responsibility

Darren Roberts QiCA MBCS, Assistant Director, ICT, Digital and Cyber Audit, SWAP Internal Audit Services

www.swapaudit.co.uk

From the outset…



- **Cyber is fundamental**
- **Demystification**
- **Non Opinion**

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Objectives for today

- Establish why we all take cyber security seriously
- What are the immediate considerations for Cyber Risk
- Why People, Process and Technology Risks and Controls are vital to establish good cyber security
- Whose responsibility is it anyway?

Why we get serious

Chartered Institute of Internal Auditors

Risks in Focus 2020

2019	2020
1. Cybersecurity: IT governance & third parties	1. Cybersecurity & data privacy: rising expectations of internal audit
2. Data protection & strategies in a post-GDPR world	2. The increasing regulatory burden
3. Digitalisation, automation & AI: technology adoption risks	3. Digitalisation & business model disruption

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

No-one wants to be the victim

Redcar Council suffered £10.14m loss due to February ransomware attack

AUGUST 5, 2020

A ransomware attack targeting the Redcar and Cleveland Borough Council's IT systems in February inflicted a financial loss of £10.14m to the Council, forcing it to seek additional budgetary support from the government.

Local Government Association

About | COVID-19 | Our support | Case studies | Parliament | Topics | Publ

Copeland Borough Council: managing a cyber attack

During the August bank holiday in 2017, Copeland Borough Council was hit by a zero-day ransomware cyber attack.

Efficiency and income generation | 09 Oct 2018

A zero-day attack means the hacker is deploying a type of virus so new it is not yet recognised by any anti-virus tools – which Copeland *did* have in place – meaning there is no way Copeland could have prevented the attack, despite their best efforts.

Lynn News

Home | News | Education | Sport | What's On | Lifestyle | Business | Jobs | Contact | Subscribe | Adve

Virus attack left council 'paralysed' as figure of £3,000 raised at meeting

By Ben Hardy - ben.hardy@iliffepublishing.co.uk
Published: 15:38, 13 July 2020 | **Updated:** 15:39, 13 July 2020

Swaffham Town Council may have to pay upfront costs of nearly £3,000 following a computer virus attack in April.

The attack was said to have left council staff "paralysed" for three days from April 22, and has been described as a "big problem".

Myth - it will never happen to me

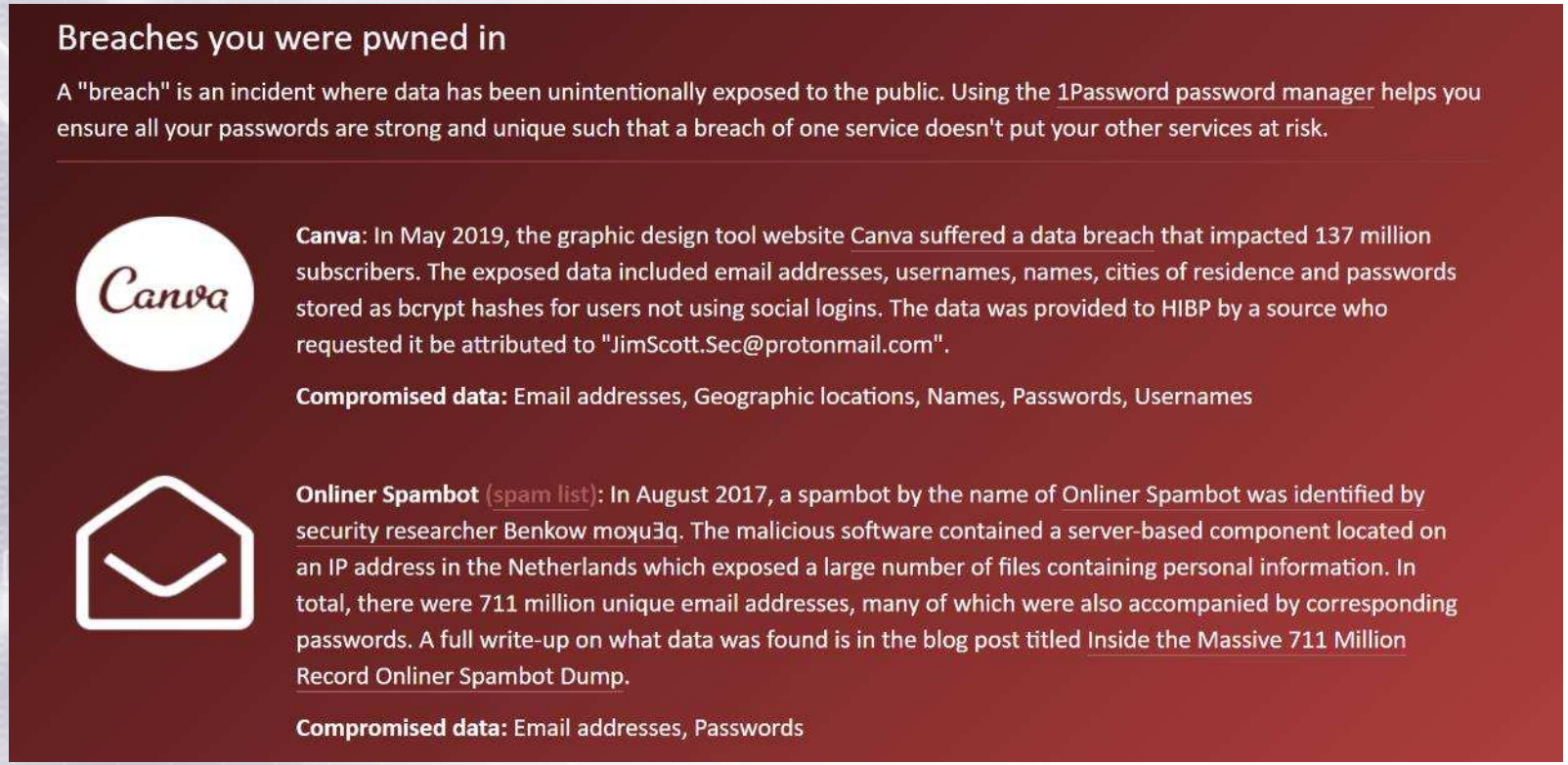
#1 You are going to get or have been exposed to a breach (https://haveibeenpwned.com/)

#2 The human factor is the weakest link

#3 Don’t rely on software to protect you

Not promoting a culture of fear - promoting a culture of compliance

Even the ICT Auditor can get “pwned”



SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Immediate considerations on cyber risk

Cyber Threats

Regulatory and Legislative

Business Continuity

Emerging Technology

Cyber Threats – The Outcomes

Monetary Outcome

Theft/sale of data

Scam or Fraud

Kidnap and Ransom

Malicious Outcome

Major Disruption

Leaks or Whistle Blow

Guerrilla Reasoning

Accidental Outcome

Data Breach

Enabler for a Cyber Attack

Regulatory and Legislative


ico.
Information Commissioner's Office

The UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

Home | Your data matters | For organisations | Make a complaint | Action we've taken

About the ICO / News and events / News and blogs /

Gloucester City Council fined by ICO for leaving personal information vulnerable to attack

Date 12 June 2017
Type News

The Information Commissioner's Office (ICO) has fined Gloucester City Council £100,000 after a cyber attacker accessed council employees' sensitive personal information.

The attacker took advantage of a weakness in the council's website in July 2014, which led to over 30,000 emails being downloaded from council mailboxes. The messages contained financial and sensitive information about council staff.

Financial

Reputational


ITPro.

Business | Cloud | Hardware | Infrastructure | Security | Software | Technology | Resources | .co.uk

NEWS Home > Security > Data Breaches

Data breaches 'have destroyed customers' trust in companies'

In the aftermath of TalkTalk and Ashley Madison hacks, people are less likely to give firms their data

High profile data breaches have decimated consumers' trust in companies, according to a survey by security firm FireEye.

Almost three-quarters of 1,000 UK respondents told FireEye they would not use services from organisations who lost their data in cyber attacks, and nearly two-thirds of people now trust companies a lot less after the torrent of high profile hacks that hit businesses last year.

Business Continuity

Hypothetical Scenario:-

Your main finance and payroll system has been subject to a ransomware attack. You are unable to access to sensitive data and critical business processes. You were due to pay staff in the monthly salary run in 2 days time.

What would you do?

So, what if you could not get access to the system for:-

- 1 day
- 1 week
- 1 month or beyond
- Or…do you pay the ransom?

Difficult Decisions

RISK MANAGEMENT / FRAUD & PRIVACY 2020

Should you pay a ransom?

Paying to get stolen data back following a ransomware attack often seems the only course of action, but you may pay double in the long run

BY EMMA WOOLLACOTT – AUGUST 20, 2020

RCNT.EU/R3A7P

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Emerging Technology

BLOCKCHAIN

5G

INTERNET OF THINGS

3D PRINTERS

BIG DATA

DRONES

ARTIFICIAL INTELLIGENCE

ADVANCED MATERIALS

QUANTUM

ROBOTICS

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Cyber Security Awareness Eco System

PEOPLE

GOOD CYBER HEALTH

PROCESS

TECHNOLOGY

People Risks

P E O P L E

- Weakest Link – they can let attackers in rather than the attacker breaking in
- Social Engineering
- Phished and Spoofed
- Cyber Auditors are quickly becoming experts in Human Psychology
- Mitigate against 4 types of user behaviour

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

Social Engineering

FEARS

NOT WANTING TO QUESTION

DESIRE TO HELP

RESPECT

NAIVETY

NOT WANTING TO BE A NUISANCE

TRUST

Social Proof

If we don't know to behave, we will mimic others.

You may well be aware of something but still behave in a certain way

People Controls

P E O P L E

- Training and Awareness
- Embed Security by Design
- Everyone fully engaged with all processes
- Culture of Compliance owned from the top
- Aware of Outcomes… which need to be enforced

Process Risks

PROCESS

- Poor, impractical or non-existent policy framework
- Reckless use of devices
- Service Management Processes are not security by design eg: Joiners, Movers and Leavers
- There's a Security Incident. What next?
- Don't know what you are protecting
- Information quality and management

Process Controls

PROCESS

- Well defined, practical, approved, enforceable and managed framework of policies
- Robust Service Management Processes – application of security updates and patches, integrated HR.
- Standard Security Builds – Hardware, Software and Cyber
- Security Incident Management
- Business Continuity Management – Back up systems and data with recovery processes
- Robust approach to Information Governance and Management

Secrets – so many secrets

What does your phone and it's installed apps know about you:-

- Location – sometimes quite precisely
- Personal Preferences
- What you like posting and sharing
- Your internet browsing history and cookies
- Data Aggregation within Apps – date and location stamps

Technology Risks

T E C H N O L O G Y

- Infrastructure design including network
- Technical security solutions at network perimeters and on devices not managed or non-existent
- Configuration of security devices are not appropriate to security requirements
- Amount of supported technology solutions not supported by appropriate resources
- Logging and monitoring may be poor and/or non-existent
- Over-reliance on the 3rd party supplier or provider

Technology Controls

T E C H N O L O G Y

- Well designed dynamic infrastructure that meets the needs of the authority
- Appropriate technical security solutions at network perimeters and on devices dynamically monitored and updated
- Configuration of security devices are subject to technical analysis and review
- Logging and monitoring has been defined and is used by inform future security decisions
- Mutual understanding between providers on technology used to embed security

Whose responsibility is this?

ICT Manager

Chief Executive Officer

Operational Staff

Elected Members

Service Managers

Head of Information Governance

SWAP
INTERNAL AUDIT SERVICES
Assuring – Improving – Protecting

It is everyone's responsibility

ICT Manager

Chief Executive Officer

Operational Staff

Not promoting a culture of fear - promoting a culture of compliance

Elected Members

Service Managers

Head of Information Governance

Promotion of culture of compliance?

Not promoting a culture of fear - promoting a culture of compliance

- Low on new solutions
- Fundamental risks not being addressed
- Payloads of Cyber Crime getting more sophisticated….
- …but the technology to initiate them is not.

Conclusion

Champions Network

More positive cyber and digital attitudes

Champions network promotes a 2-way approach feeding back on gaps

Embed culture of compliance at induction

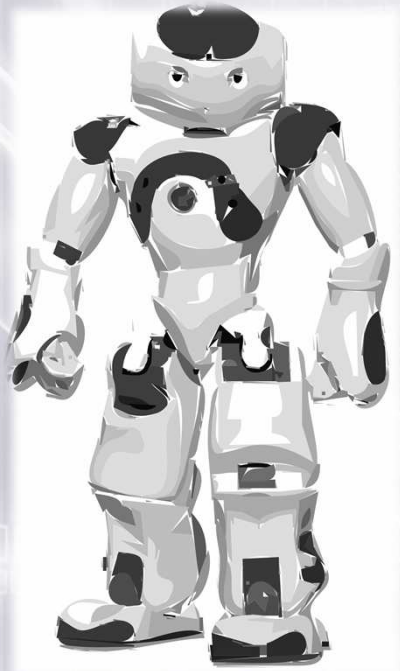
Be realistic, don't overwhelm, prioritise on what you want to achieve

Use scenarios and hypothesis - be brave.

Search: "Security Champions Playbook" on OWASP

Not promoting a culture of fear - promoting a culture of compliance

Over to you…



A better word than Cyber?

Darren Roberts QICA, MBCS

ICT, Digital and Cyber Assurance | ICT Auditor (QiCA) | BCS Professional (MBCS) | Chair of BCS IRMA SG |

LinkedIn

Cyber is for everyone

Questions

Darren Roberts QiCA MBCS
darren.roberts@swapaudit.co.uk
Assistant Director, ICT Audit Team
SWAP Internal Audit Services
28th April 2021