# David Cowan
# ICT Manager
# Copeland Borough Council

Copeland
borough council
*Proud of our past. Energised for our future.*

# Protecting Systems And Data From Potential Attacks By Investing In Cyber Security

www.Copeland.gov.uk

# Background

- Copeland Borough Council is a very small local authority nestled on the west coastline of Cumbria, largest town is the port of Whitehaven.
- We have an Elected Mayor, 55 elected members and 218 permanent staff.
- Primary employer within the local authority area is the Nuclear Decommissioning Authority at Sellafield.
- In 2017, the council suffered what is believed by many to be the most devastating Cyber Attack to ever occur within UK Local Government and at the present time 2019 the Council remains in recovery mode.

Carlisle
Maryport
Workington
Whitehaven
Penrith
North Pennines AONB
Keswick
Lake District National Park
M6
Windermere
Kendal
Yorkshire Dales National Park
Barrow-in-Furness
Lancaster
M6
Forest of Bowland AONB

# Cyber Attack 2017

Copeland borough council
Proud of our past. Energised for our future.

- Despite having fully updated and active Anti-Virus software in place, the council systems were hit by what is known as a **"zero day" virus** and therefore the active Anti-Virus software did not recognise the virus and did not prevent the attack
- The **cyber attack** was also conducted over a **bank holiday weekend**, providing a long period of time before discovery and the start of the Council's response. This helped maximise the impact of the virus to Council IT servers.
- By the point of discovery and the commencement of containment actions the Council was at the point of having **lost nearly all key IT systems**, all network services and near 100% of the end-point devices such as desktops and laptops.
- As soon as our partners in our shared service initiatives were informed of the problem, the Council was also **immediately cut-off from all access to shared services** to all partners to prevent cross-contamination.
- The Council found itself in a position where **technology effectively no longer existed**.

# Cyber Resilience

- The Council found itself in a position of **assuming** the **internal IT team would just sort** everything quickly, but this quickly became apparent that this was not a realistic expectation.

- Copeland has a very **small IT team**, the scale of total loss suffered over-whelmed what IT resources were in place and extra IT help needed to brought in very quickly to help recovery.

- The Council also discovered that existing **emergency plans** and **business continuity plans did not cater sufficiently for a scenario of 100% IT loss,** and in a scenario where you no longer have email or IT systems to communicate, the Council found itself in needing to setup a new daily physical meeting of key managers to deal with the new scenario.

- The **IT network was compromised** and it took many days just to regain control of some pockets of the network. It was at this early point in the recovery that the most significant impact of the attack was discovered, the **system backups in place were compromised**, so a straight-forward restore of the IT systems to a state prior to the Cyber attack was not an option

- The **IT infrastructure was going to need to be rebuilt from the ground up** and that meant a long period of time (months) with no IT systems at all.

# Cyber Resilience - Impacts

- Very close to all Council activity had to **revert to pen and paper**, even the ability to pay Council staff was lost and the authority was forced to revert to organising paper cheques to pay staff wages.

- Staff where possible were dispersed to work in non-council locations and where feasible neighbouring local authorities, if that enabled them to have access to relevant IT systems external to the Council.

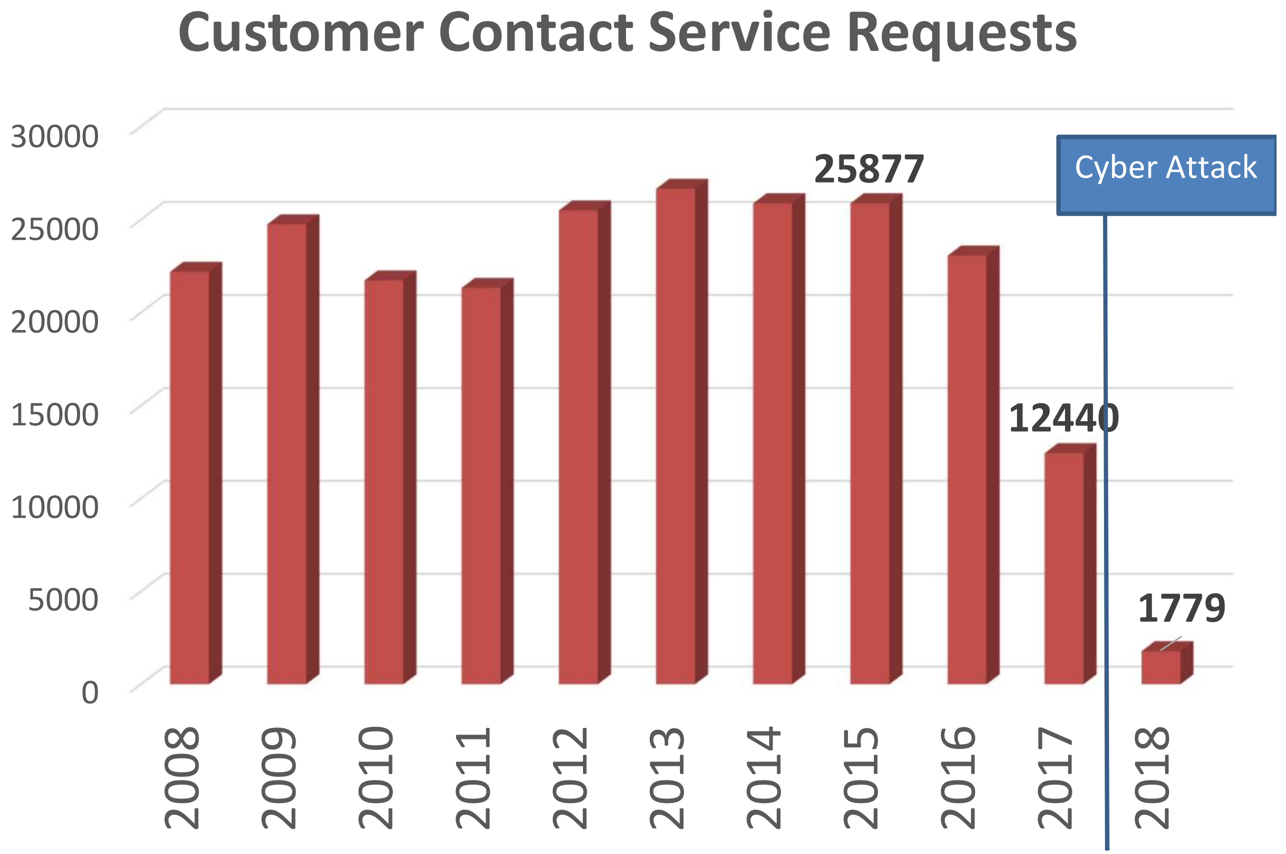
- Approaching 2 years after the initial event, **Copeland remains in recovery mode** with some IT systems still in the process of undergoing remediation.

- Leaving aside the costs of lost productivity and the enormous service impacts, this one Cyber attack has to date **cost a minimum of £2.5 million pounds** and the recovery costs continue. Total council budget for all services is circa £9m per annum

- Our customer service IT systems recorded an average of 25,000 processed service requests per annum prior to the Cyber Attack

# Cyber Resilience - Impact

Proud of our past. Energised for our future.



# Key Learning Points

- **Chief Exec and Leadership Team Buy-in** and Active Support is Crucial

- **Be Prepared**
  - Make sure your Cyber Defence Investment is Appropriate **AND** Sufficient
  - Make sure you have plans for a total IT loss scenario
  - **Do not default to assuming IT is Safe** – Ask and Verify.

- **Data and System Security** is the **Responsibility of All Staff**
  - Everyone has a Stake in Data and Systems Being Safe and Secure
  - **Don't forget your Service Partners and Suppliers**

- As the Systems needed to be rebuilt decisions were taken to adopt a **Cloud Hosted First** approach to empower a **future Agile workforce** to avoid a repeat of this scenario.
  - Where key IT systems were completely external to the Council, such as hosted solutions, the Council was able to utilise these systems.
  - Control your deployed end-point devices – Laptops, Phones, Tablets, IoT Devices

# Key Advice

- **Take Cyber Defences Seriously** and **Be Prepared**
- Well maintained and configured Firewalls and Supporting Network Devices
  - Ensure all points of ingress and egress are covered
- Forced **Regular vulnerability patching** across the entire estate.
  - Copeland force patch at least once per week, and will push key security vulnerability patches out the same day when required, but only after testing the patch on our lab kit.
- **Defence in Depth**
  - Make sure you are not vulnerable to a single point of failure
  - Zone and Segment the network to control the network traffic flows
- **Backup in Depth**
  - Follow an appropriate regime for the data
  - Backup at least once per day, with transaction log backups inter-day where appropriate.
  - Do not rely on single location backup
    - Copeland backup all data to 3 locations per day – 2 onsite, 1 offsite.
  - Ensure users are not saving files to any location that is not being backed up
    - Files should not be saved on local hard drives
- **Follow Advice** From **National Cyber Security Programme**

# So We Are Safer In The Cloud ?

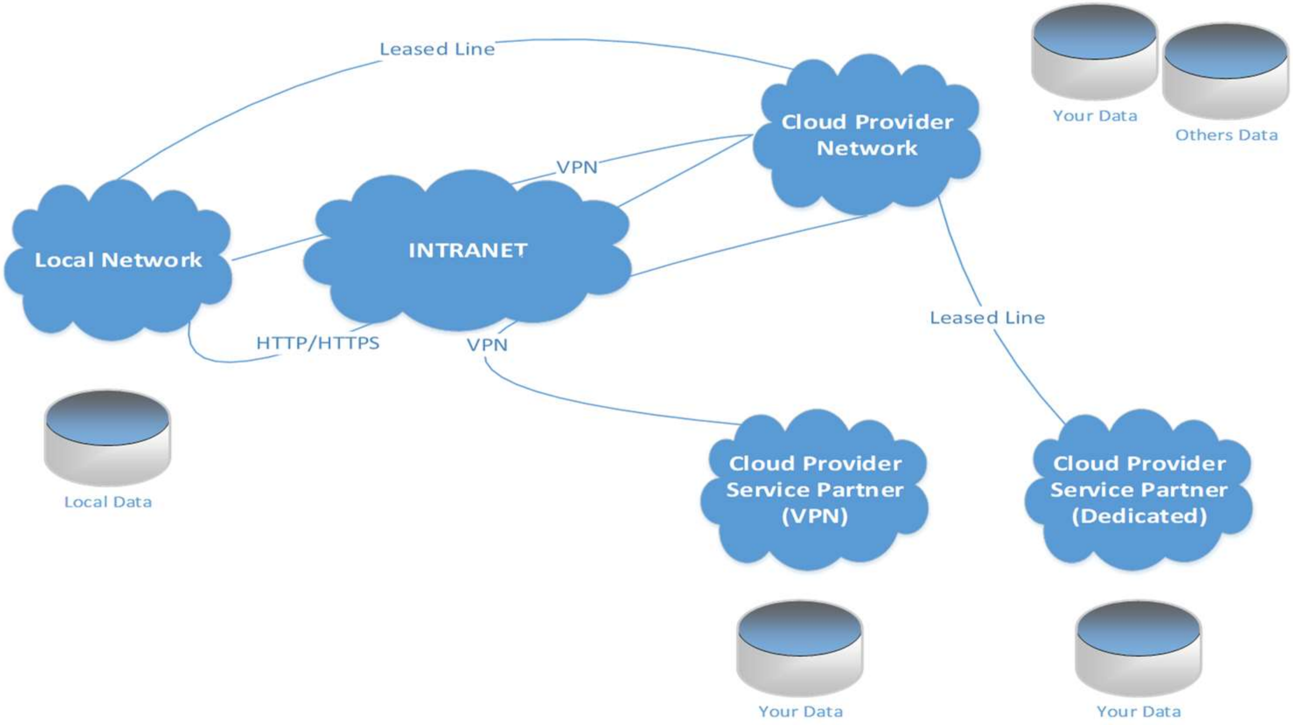
- Very Misleading and Widespread misconception, it very much depends on what you have done to protect yourself in the Cloud.

- **Basic Cyber Risk Profile (Premises vs Cloud)**
    - Very hard to compare, but the risk surface area for a potential Cyber Attack before applying any measures is higher by its nature and **therefore more <u>NOT</u> less** needs to be done to protect Cloud systems.

    - Before any security measures are deployed, we explain it as:
        - Risk Locally **On Premises 5 out of 10**
        - Risk for **Cloud Hosted 8 out of 10**

    - If you running a **Hybrid Setup** – part-on site and part in Cloud, you have increased risk not reduced risk.
        - If you are running a Key System which is not 100% Cloud, it is also not 100% Agile or Resilient, it is subject to failure both On Premises and in The Cloud

# Understand Your Risk Scope



- **Supplier Information Security Assessment**
  - Conduct Full Cyber Security Risk Profile on All Suppliers AND Their Suppliers

# Supplier Information Security

- Sample Questions To Consider Asking Your Suppliers
  - Who am I entrusting with my data – do they hold verifiable certifications?
    - Think of Yahoo, LinkedIn, Facebook
  - Where is my data stored in terms of geography – Not just “in the Cloud”
  - What backup strategy is followed with my data
    - Is it Backed up and in resilient fashion
  - Is my data “encrypted at rest”
  - Is my data “encrypted in transit”
  - Is the Cloud Host wholly owned or sub-contracted out
    - If contracted out ask all the same questions of them as well
  - What Cyber defences does the Cloud provider follow
  - What security vetting do the providers staff have
  - How is the system monitored
  - Single versus Multi-Tennant – How does supplier assure separation
  - Who controls sign-on permissions
  - How long to Recover in Disaster Event

# Cyber Security Technology

- **Firewalls**
- **Anti-Virus** – all points
  - Network Ingress, Egress, All user end-points and Servers
  - Everybody uses don’t they – Do They?
- **Regular Patching** of All software
  - Allowing software to drift away from upgrades is bad news
- **Email Phishing defences** – DMARC/DKIM
  - Assuring sender is the real sender
- **Check your Logs**
  - Know what attacks/probes you are catching
  - Review daily, Take action
- **Network Zoning and Segmentation**
- **Physical protection**
  - Removable media, portable disks, physical Access to Infrastructure
- **Regular IT Health Checks and Pen Testing**
  - Consider Rotating Suppliers Each Time – Once per year is insufficient
- **Cyber Training for All Staff and Members**

# Cyber Security Technology

- **Information Classification**, supported by technology
- **Data Loss Prevention**
  - What ways can someone remove copies of your data
- **Cloud Access Security Broker**
  - Do you have control of who in your authority can access what?
- **White-listing** all Browser Cloud Access
  - Protective DNS service (National Cyber Security Centre provide service)
- **Advanced Log Collection**, filtering and monitoring
  - Patterns Searching
- **Intrusion Detection**
  - Has someone actually got in despite your Cyber defences
  - Remember Copeland was hit with “Zero Day”
- **Advanced Monitoring**
  - 24x7 Active Monitoring and Alerting (SOC or Managed SIEM)
- **External, independent reviews**
  - Annual PSN Re-certification and IT Health Checks
- **Regular Drills**
  - National Cyber Security Centre is running programme of events

# Thanks For Listening

David Cowan

David.cowan@Copeland.gov.uk

National Cyber Security Centre

https://www.ncsc.gov.uk/

National Cyber Security Centre
a part of GCHQ