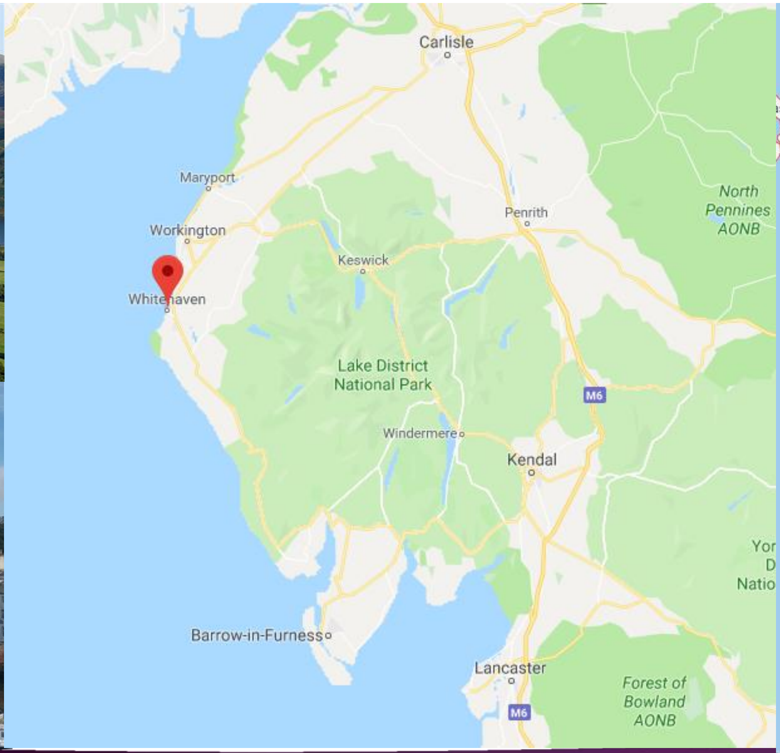
Copeland borough council

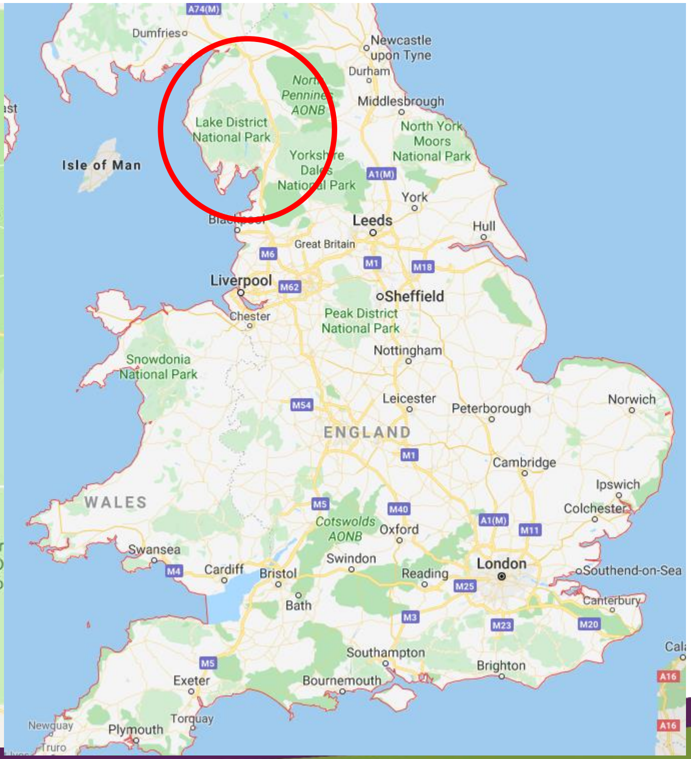
Proud of our past. Energised for our future.

Response and Recovery from a Major Cyber-Attack Case Study

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, 33 elected members and 290 staff.

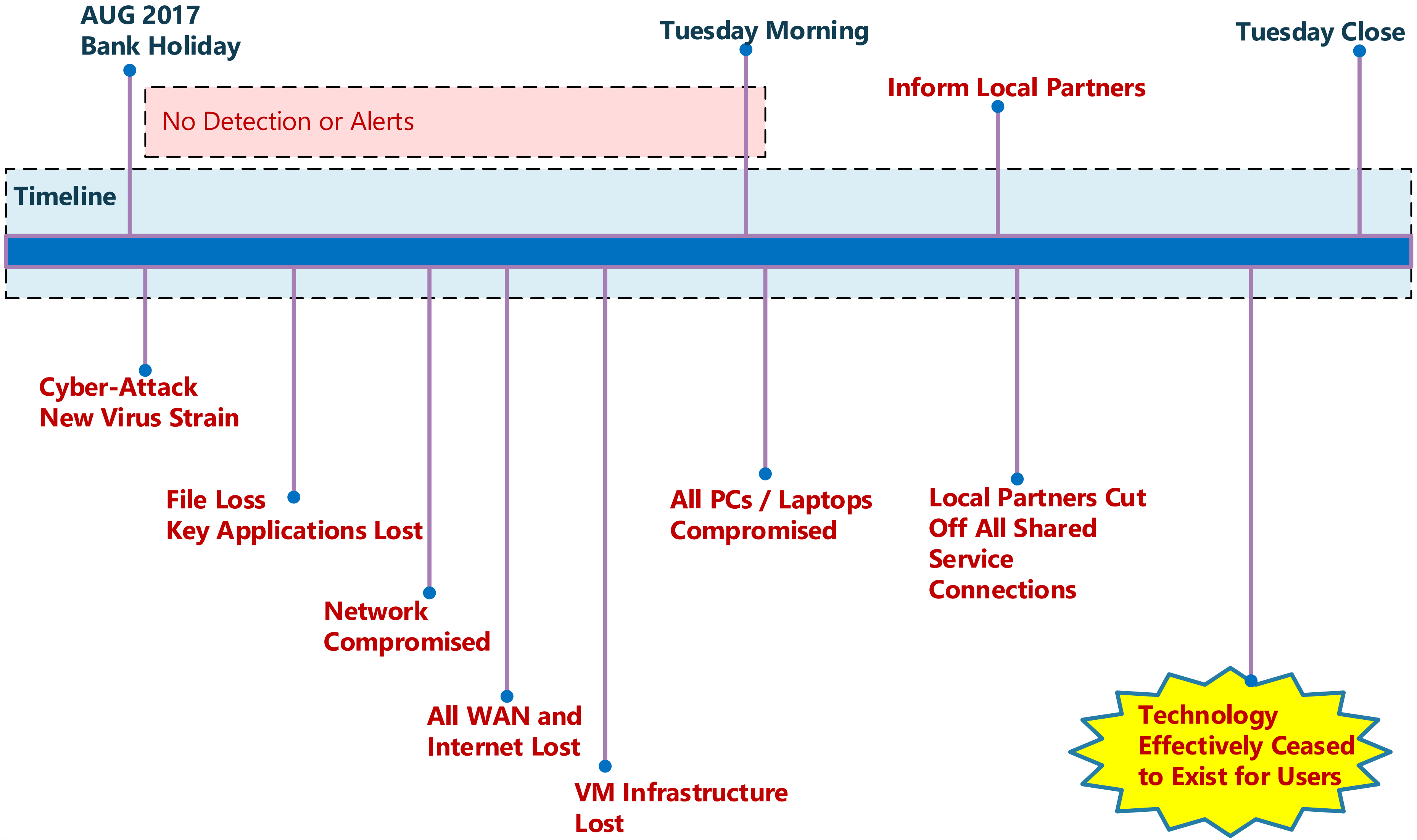




Largest Nuclear Site in Europe

- Primary employer within the local authority area is the Nuclear Industry.
- Sellafield, largest, most complex and congested nuclear site in Europe. Two square miles of science, innovation and engineering.

Cyber Attack 2017



AUG 2017
Bank Holiday

No Detection or Alerts

Tuesday Morning

Inform Local Partners

Tuesday Close

Timeline

Cyber-Attack
New Virus Strain

File Loss
Key Applications Lost

Network
Compromised

All WAN and
Internet Lost

VM Infrastructure
Lost

All PCs / Laptops
Compromised

Local Partners Cut
Off All Shared
Service
Connections

Technology
Effectively Ceased
to Exist for Users

Cyber Attack 2017

- Despite having fully updated and active Anti-Virus software in place, the council systems were hit by a new **“zero day” ransomware virus strain** and therefore the active Anti-Virus software did not recognise the virus and did not prevent the attack

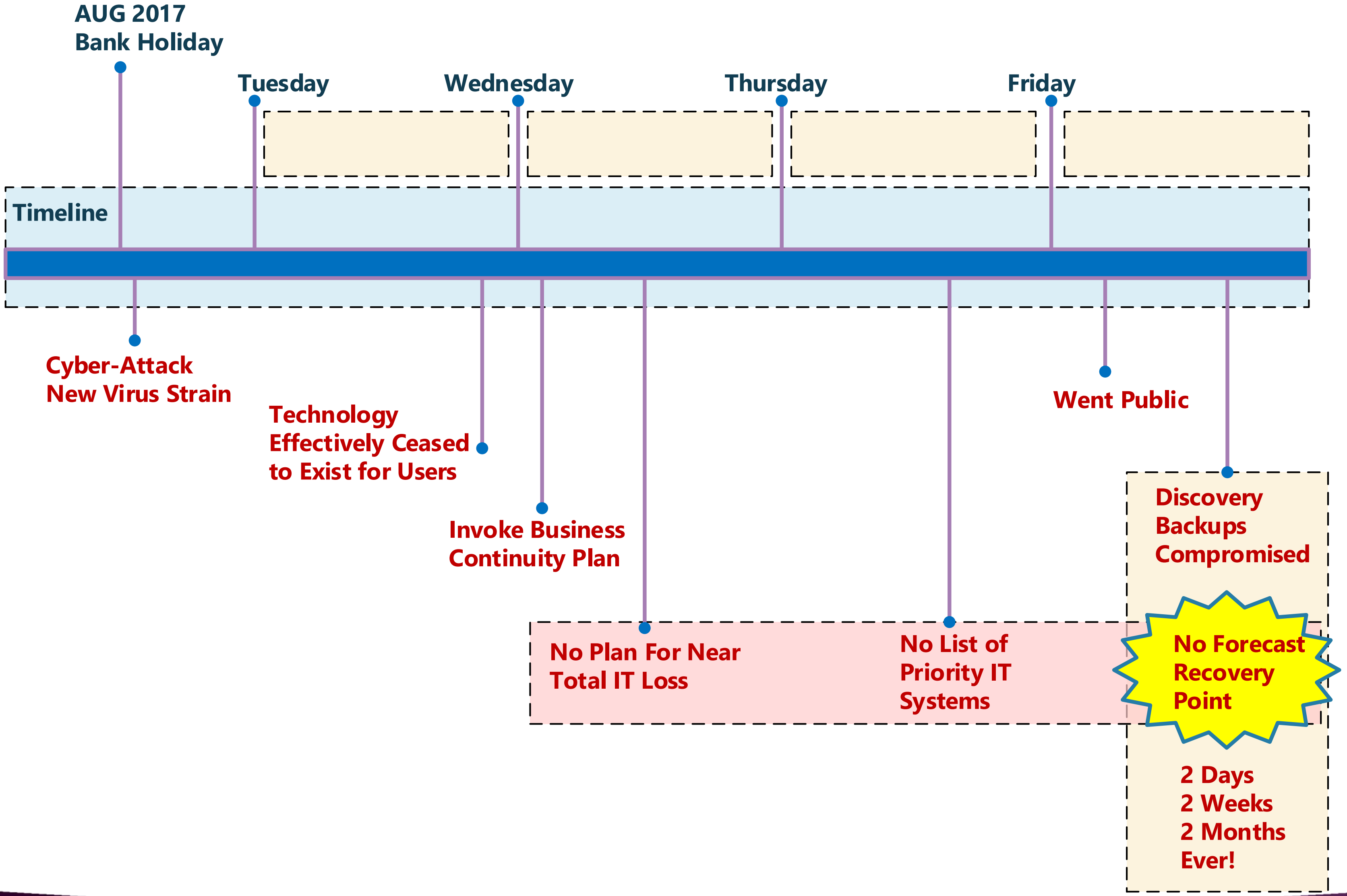
- The **cyber attack** was also conducted over an August **bank holiday weekend**, providing a long period of time before discovery and the start of the Council’s response. This helped **maximise the impact** of the virus to Council IT servers.

- Before containment actions could be started, 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.

- When our shared service partners were informed, 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 Attack – IT Team Will Sort It



AUG 2017
Bank Holiday

Tuesday

Wednesday

Thursday

Friday

Timeline

Cyber-Attack
New Virus Strain

Technology
Effectively Ceased
to Exist for Users

Invoke Business
Continuity Plan

No Plan For Near
Total IT Loss

No List of
Priority IT
Systems

Went Public

Discovery
Backups
Compromised

No Forecast
Recovery
Point

2 Days
2 Weeks
2 Months
Ever!

Cyber Attack – IT Team Will Sort It

- 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 be brought in quickly to help recovery.

- **Chief Exec asked IT Manager** when it would be fixed, expecting an answer measured in hours or a couple of days, first bombshell response was **maybe never**!

- 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.

Invoke Business Continuity Plan

- **Corporate Business Continuity Plan Activated**

- **Paper copies** of the Business Continuity Plan lodged with key managers helped

- However, The Council 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 **ransomware messages** demanded millions, law enforcement **advised not to pay.**

Impact – The Nightmare Begins…

- All **computers switched off**, unable to print, unable to access <u>anything</u>
- **No Finance system**
  - 2 weeks until pay day,
  - 1 week to pay for diesel for waste collection services
- **Local by-election called**
  - No access to Electoral Register, or Elections system
- **Land searches backing up and housing market grinding to a halt**
  - Families forced to stay in hotels
- **Senior Leadership Team**
  - Business as Usual – non existent!
  - Impossible to understand what has happened, or, if and when we will switch on!

Cyber Resilience – Recovery Start

- Nearly all Council activity had to **revert to pen and paper**, even the ability to pay Council staff was affected.

- **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.

- Over **2 years** after the initial event, **Copeland remains in recovery mode** with some IT systems still in the process of undergoing remediation. Some data has been subject to total loss.

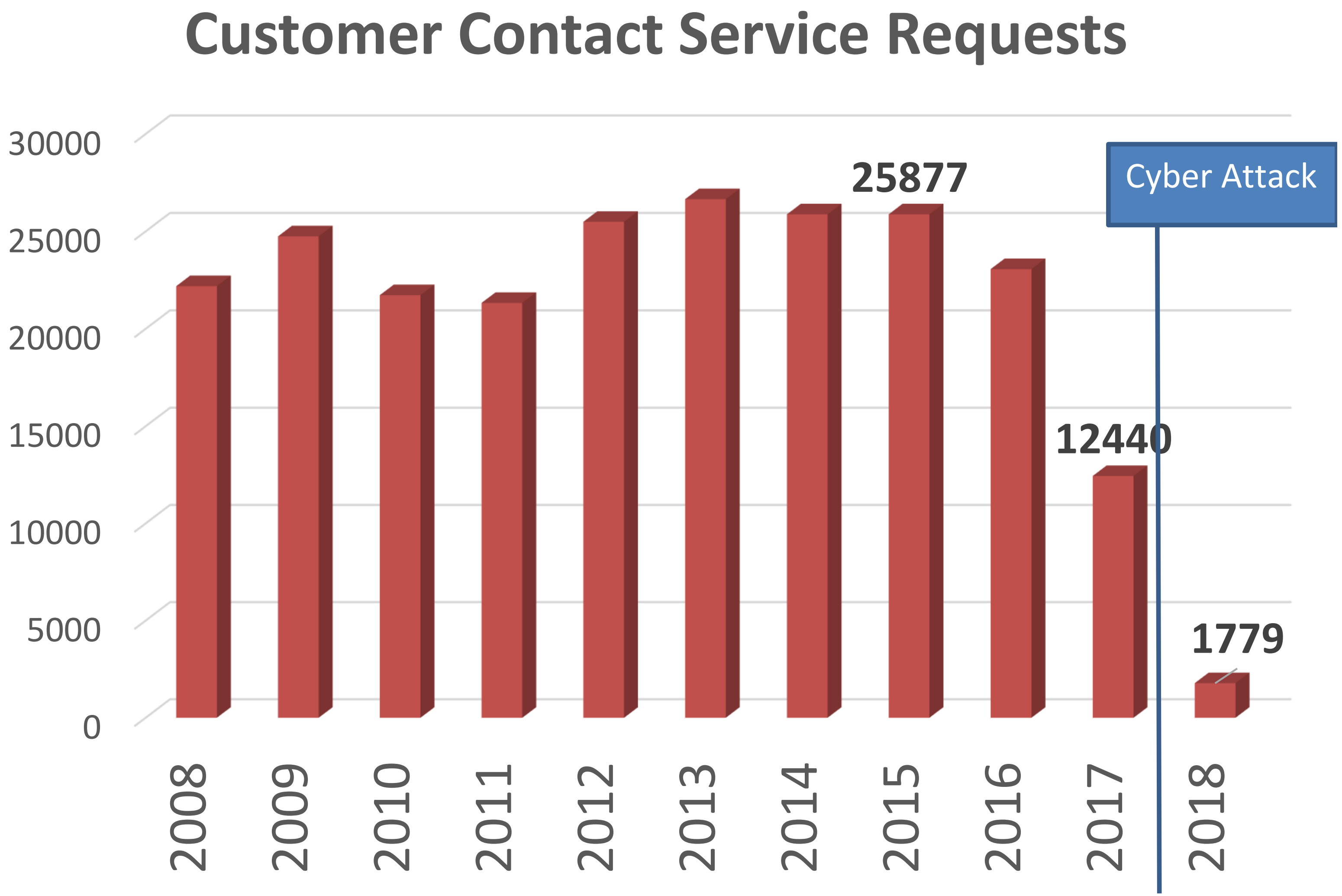
- Leaving aside the costs of lost productivity and the enormous service impacts, this one Cyber attack has to date **cost over £2.5 million pounds** and the recovery costs continue. Total council budget for all services is circa £9m per annum

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

Tracking Public Interactions - Impact

Copeland borough council

Proud of our past. Energised for our future.



Impact on People

- Devastated, Angry, Frustrated
- Despondent - going back in time, years of effort gone!
- Challenging information given and decisions taken
- Doubted we would ever recover, some considered leaving
- Confidence in IT service lost, IT staff literally working around the clock, others struggling to know what to do each day!
- Counselling offered
- Members
- Leadership was key, but answers didn't come easily….
  - Priorities very difficult

Reputational Impact!

- Early decision to go public, worked hard to stop this from becoming old news - even now!
- Partners automatically sent invoices – had to warn them fast, (email addresses sold recently on the dark web!) – Ongoing issue
- This was not going to be a quick turnaround – needed media to get the message out!
- Partners locked us out - high risk!
- We were in lock down and couldn’t hide it!
- ICO were a constant – fear of a fine!
- Over time, accused of using cyber attack as an excuse – short memories!
- Praised for our open and transparent approach!

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**

- **Make time to manage your storage**
  - Every file has a recovery cost

- **Make Your Cyber-Security Protocols Clear**
  - Train Members and Staff regularly
  - Agree the rules and stick to them

Key Learning Points

- **Know Your IT Assets, Organisational Configuration and Reliance**
  - Consistency aids recovery
  - Ensure all key systems and data have Business Owners
    - What data do they use, where does it come from, how does it flow, who else uses it
  - Make Sure Key Data is in Verified Backup and In-Depth

- **Governance**, Oversight and Verification of **IT in the Enterprise**
  - IT inform business decisions – not make them. Business staff do not make IT decisions without appropriate IT input and advice

- **Do Not Underestimate How Long Recovery Will Take and Lasting Impact on All Involved**

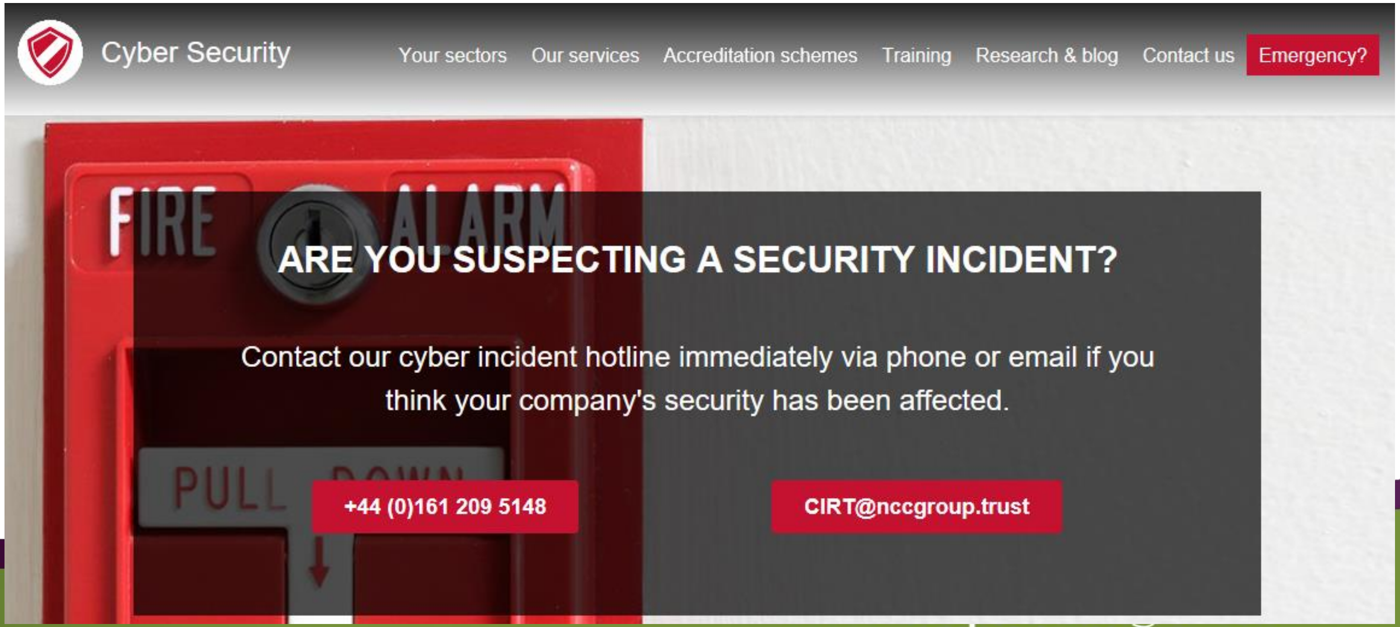
Key Advice

- **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
  - Make sure Cloud and Hosted data services are being backup up properly
- **Follow Advice** From **National Cyber Security Centre Programme**

Key Advice

- **Make sure you have a "Phone a Friend"**

- Know the organisations you could reach out to for help before you need them and embed in your emergency planning in a sensible fashion.
    - Key Supplier Contacts
    - Key Partner Organisation Contacts
    - NCSC
    - Cyber Crime Units
    - Trusted Organisations who run "Cyber Incident Services"
        - NCC Group
        - Claritas
        - etc



ARE YOU SUSPECTING A SECURITY INCIDENT?

Contact our cyber incident hotline immediately via phone or email if you think your company's security has been affected.

+44 (0)161 209 5148

CIRT@nccgroup.trust

Thanks For Listening

David Cowan

David.cowan@Copeland.gov.uk

Full Case Study on Resilience Direct
Prepared by MHCLG – National Cyber Security Programme – Local

https://collaborate.resilience.gov.uk/CyberHub/home/201/Copeland-Borough-Council-Cyber-Incident-and-Recovery-Case-Study-Report

Ministry of Housing,
Communities &
Local Government

Think Cyber
Think Resilience
Building Resilience Together