Copeland borough council

Proud of our past. Energised for our future.

Major Cyber-Attack Lessons Learned Reviewed in Light of Covid Copeland Case Study

Covid and Copeland Cyber Lessons

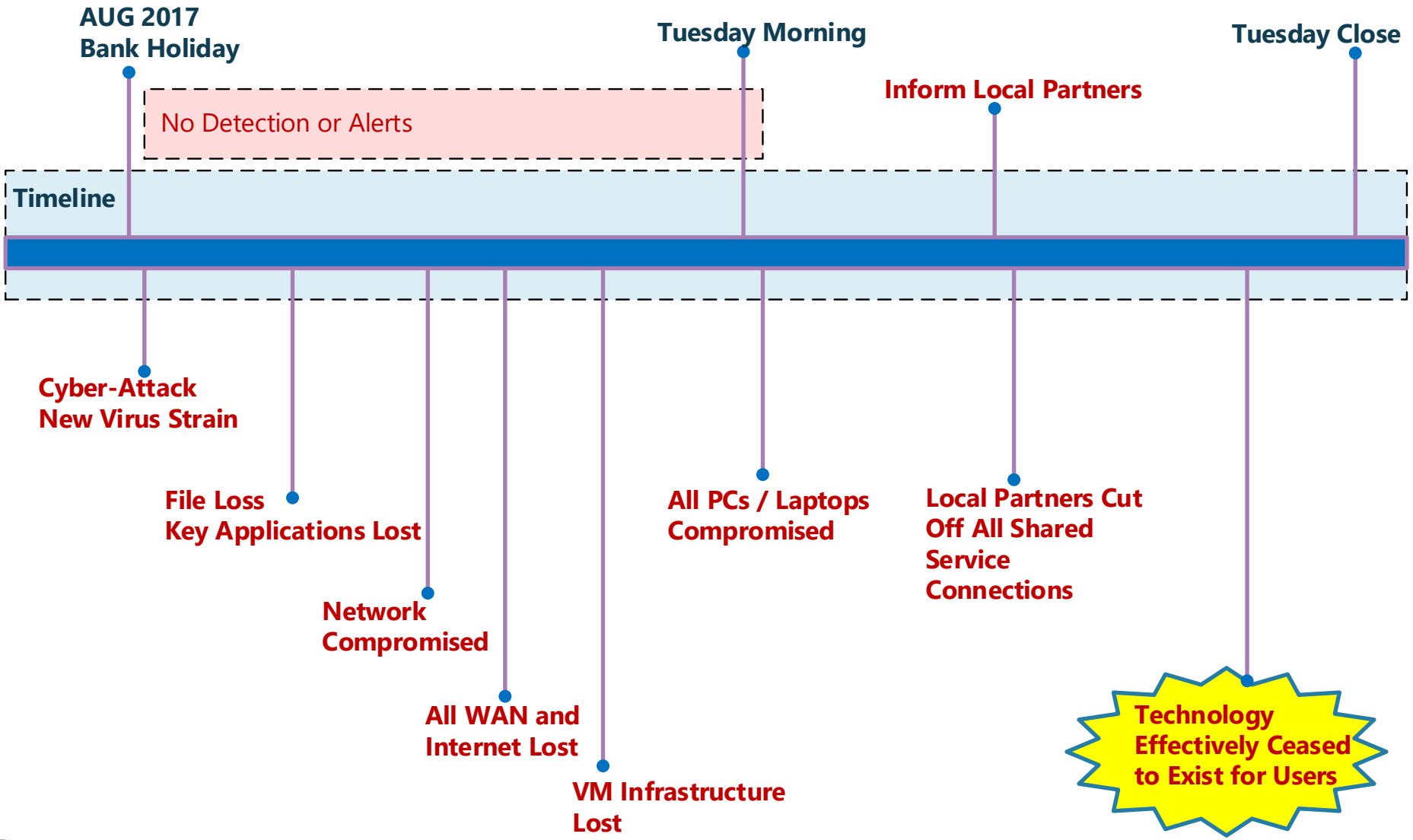
- Quick Reminder of Copeland Attack and Lessons Learned
- Our Cyber Related Challenges During Covid
- How Did Our Cyber Attack Lessons Learned Influence Response

The Headlines!

- **Previously over a August Bank Holiday**, Copeland Council suffered a **Devastating Cyber-Attack** that took many months to recover from.

- Combination of attacks believed to have started with a "**Brute Force Remote Desktop Attack**" ultimately led to "**Zero-Day Ransomware**" - active Anti-Virus software did not recognise or stop the ransomware and the combined active cyber defenses could not stop the attack.

Cyber Attack or a “glitch”!



Invoke Business Continuity Plan

- **Corporate Business Continuity Plan Activated.**

- **Paper copies** of the Business Continuity Plan lodged with key managers helped, now mandated for Senior Team at Copeland.

- 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 and we didn't.**

Impact – The Nightmare Begins…

- All **computers switched off**, unable to print, unable to access anything
- **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/animals in kennels
- **Senior Leadership Team**
  - Business as Usual – non-existent!
  - Impossible to understand what has happened, or, if and to communicate to staff, elected Members and the public
- **Staff turning in to work – but can't do anything!**

Know Your Impacts, Exposures and Prepare For The Worst

Key Learning Points

- **Common Recurring Themes from multiple large-scale major cyber attacks**
  - **Senior Leadership**
    - Chief Exec / Senior Leader sets the tone Before, During and After (Controls Recovery Priority)
  - **Be Prepared**
    - Protect Adequately
    - Have a Cyber Incident Plan and Exercise it on Regular Basis
  - **Know Your Assets**
    - Critical to Protection, Response and Recovery
  - **Backup Strategy**
    - NCSC 3-2-1 minimum but you might need more …
  - **<u>Do Not</u> Underestimate How Long Recovery Will Take**
    - Lasting Impact on the Organisation and All Involved

All These Lessons Are Detailed In The Full Case Study

Covid Challenges

- **Workforce Only Partly Enabled for Remote Working (circa 55% Enabled)**
  - Just as we did post cyber attack we had to sit down with Senior Leadership and make priority calls on how we re-distributed kit while we sourced more.
  - This means being really clear which departments and which users are “key” – the answer is never everybody
  - It took us about 4 weeks to source and deploy remote working kit to 100% of our work force

- **NCSC Warned of Increased Cyber Risk to Sector but Huge Pressure to Setup New Solutions**
  - Business leads needed to be reminded about risks and not just use any technology
  - Chief Exec crucial in maintaining our cyber policies and stance
    - We held to MFA on all cloud solutions despite pressure not to
    - We held to no uncontrolled unsecure connections to our network
    - We held to no BYOD or use of personal devices

- **Some of Our Key Suppliers Let Us Down, Some Really Helped – Just Like Cyber Attack Recovery**
  - Lockdown suddenly became a big reason why some failed, while some had the resilience to continue
  - Our main phone system died on us in the first week of lockdown
    - We deployed a new cloud based phone system in less than 24 hours (Value of Partners)

Covid Enablers

- **Business Continuity Cyber Planning**
  - Previous Business Continuity Planning business reviews and Council-wide exercising massive help
  - Really helped our management be prepared on how to run with minimum technology
    - Mainly in those early days when we lacked business systems to deal with demands
  - Our senior team knew the impact of any successful cyber attack against our systems

- **Cloud-Based Collaboration Platform (Voice, Video, Messaging, File Sharing, etc)**
  - Copeland was just about to begin a 6 month rollout of Cloud Collaboration platforms, we deployed the Voice and Video elements in a matter of hours and Structured File Sharing within a few weeks
    - This enabled communication key internal and external communication
    - This provided independence for many staff enabling home-working
    - Enabled Council Remote Meetings

- **Our Improved Technology and Security Tooling Post Cyber Attack Enabled**
  - Split tunnel VPN and enhanced device protection meant No backhaul of VPN network traffic
  - Our Cloud adoption and security tools gave us confidence to quickly assess the risk of other Cloud SaaS offerings and adopt solutions within our risk appetite
    - Included new remote working enabler solutions such as work force tracking and zero touch building occupant recording

Key Learning Points

- **Common Recurring Themes from multiple large-scale major cyber attacks**
  - **Senior Leadership (Proved Key to Help Us Respond Without Dropping Cyber Stance)**
    - Chief Exec / Senior Leader sets the tone Before, During and After (Controls Recovery Priority)
  - **Be Prepared (Proved Key in Helping Our Business People Being Prepared)**
    - Protect Adequately
    - Have a Cyber Incident Plan and Exercise it on Regular Basis
  - **Know Your Assets (Helped Us Know What We Had and How to Prioritise and Best Respond)**
    - Critical to Protection, Response and Recovery
  - **Backup Strategy (Solutions in Place Fully Automated Helped Us Work Remotely)**
    - NCSC 3-2-1 minimum but you might need more …
  - **<u>Do Not</u> Underestimate How Long Recovery Will Take**
    - Lasting Impact on the Organisation and All Involved **(Our People Support Was Called On Again)**

Covid Response in Light of Cyber

- **During Covid We Increased Our Cyber Stance, We Did Not Lower Our Bar Because of Covid**
  - **We Rapidly Risk Assessed All Solutions**
    - We rejected a number and put in alternative controls where we felt required
  - **We Innovated With Introduction of New Solutions to Support Council Response**
  - **Chief Exec Message – "Take your problem to ICT, not your solution"**
    - Allowed us to maintain our cyber security resilience but onus on ICT to support the business with usable solutions to the problems in tight timeframes measured in hours to days
  - **During Covid we suffered an increase in attempts by cyber adversaries to attack us, but nothing disrupted our systems or our response.**

Thanks For Listening

David Cowan - David.cowan@Copeland.gov.uk

Full Case Study on Resilience Direct (Within Cyber Hub)
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