Wiltshire Council
Where everybody matters

The Cyber Impact of the Salisbury Novichok Poisoning

Stephen Vercella, Head of ICT Wiltshire Council – Dec 2019

“As the novichok poisoning incident unfolded in Salisbury in early 2018, we realised that Wiltshire had become a centre of attention worldwide. What we were slower to realise was that this interest was not restricted to the media, but also manifested itself as a **huge increase in activity to break into our systems** causing significant additional work to ensure they remained secure.”

Agenda

1. Wiltshire Council
2. 2017 – Important learning before the event
3. The initial incident
4. The incident that keeps on giving
5. Other stuff
6. Summary of impact

Wiltshire Council

- A unitary authority
- The Council's ICT department provides ICT services to Wiltshire Council and Wiltshire Police on a shared ICT infrastructure
- We support approximately 4,000 Council users and 2,000 Police users
- ICT has an establishment of 118
- Support is 24x7 but minimal coverage out of office hours
- Council currently use O365, Police do not.

2017 – Important Learning Before the Event

Cyber incident exercises with Wiltshire Police

- Where do ICT get their decision making authority?
- Use of decision models to guide and document decisions (NDM/JDM)

Poor IT Health Check

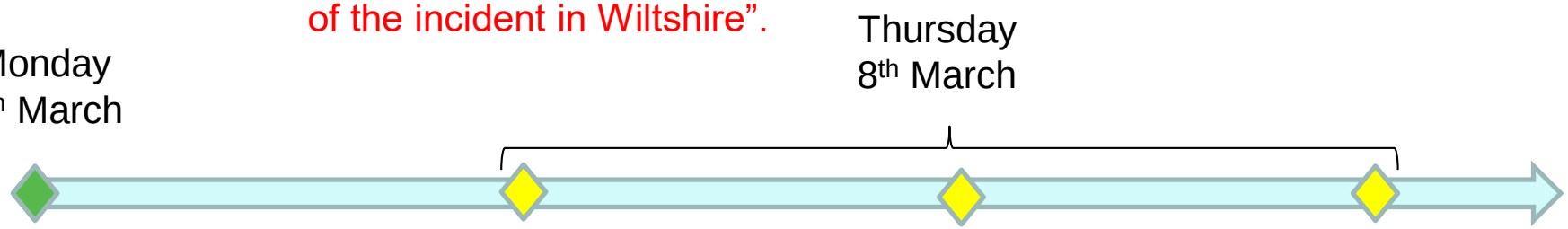
- Good understanding of vulnerabilities
- Focus on security within organisation.

Wannacry

- Development of a disconnection process.

Initial Incident

"NCSC: …increased Cyber Threat to entities involved in the investigation of the incident in Wiltshire".



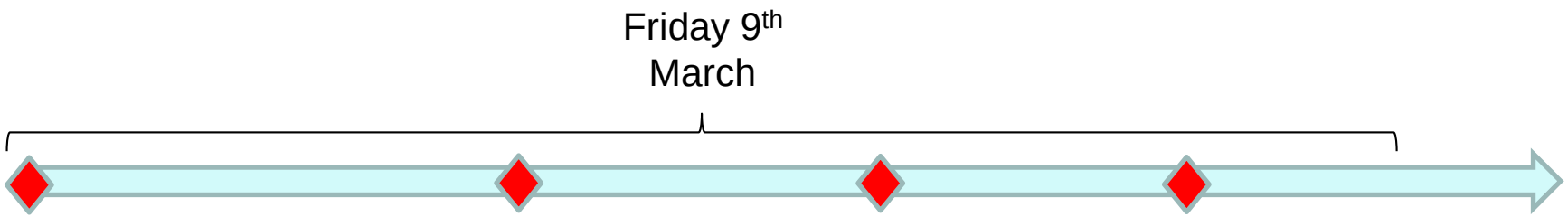
BBC News report - a man and woman have been poisoned by an unknown substance in Salisbury

Contact made with NCSC (thro Wilts Police) and lines of comms established. Possibility of disconnection considered. Possibility of disabling vulnerable systems considered

Salisbury Hospital report attempt to hack their systems. Council firewalls show unusual activity. Both originating from Russia.

Decision to continue monitoring.

Initial Incident



Council Shadow Recovery Group informed systems could be turned off if significant threat and could escalate to disconnection of all external connections.

ICT authority reconfirmed.

ICT Manager and senior technician rota established.

Internal comms prepared

High alert detected by O365 (Malware campaign)

Decision made to disable Access to email & calendar from mobile phones (significant vulnerability) causing significant disruption

Learning from initial incident - 1

Security risk is not a constant (secure or not secure), it continuously changes

- Interest in your organisation varies and spikes
- ICT systems constantly change, therefore so do their security vulnerabilities
- As a result, security risk is constantly changing

Need to react to these changes

- We shut down systems with vulnerabilities when the threat changed

Need to proactively plan for changes in risk

- When your organisation is “of interest”, the threat increases

Learning from initial incident - 2

Are processes, authorities & attitudes fit for purpose (cyber attack)?

- Is ICT authority clear? – learnt from exercise
- Can ICT disconnect at **any** time? – learnt from Wannacry
- Can you quickly put necessary out of hours cover in place (technical & management)? – learnt this in incident

Documentation

- Use of NDM to document decisions provided valuable information after the event

Learning from initial incident - 3

Business Continuity

- Business areas don’t understand their reliance on ICT very well

Initial incident - Question

Do you use your IT Health Checks, security audits, etc to prove you are secure or to understand your vulnerabilities?

The Incident That Keeps on Giving

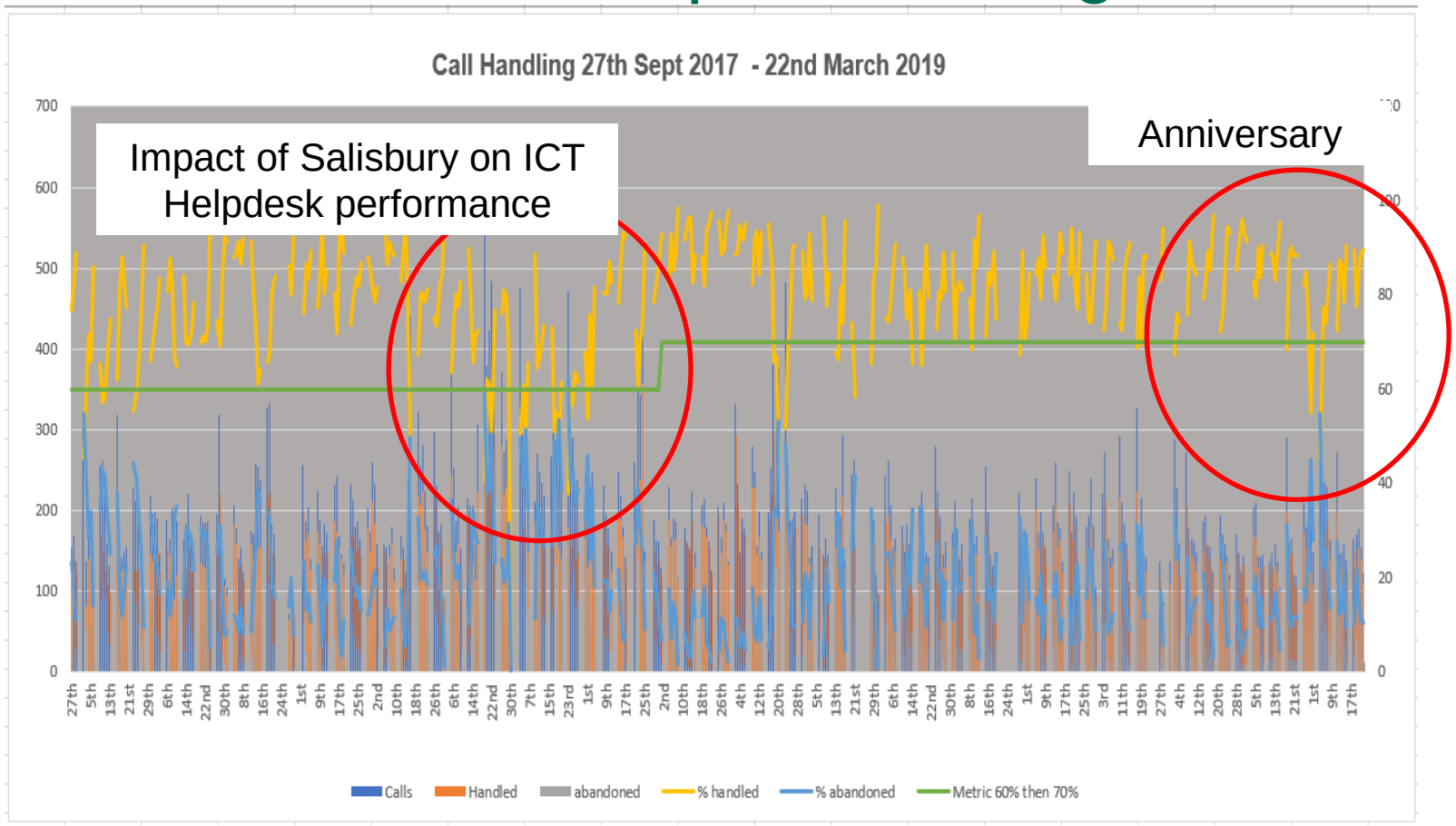
- Increased interest – Wiltshire is now known worldwide
- Led to increased attempts of unauthorised access to O365 accounts
- Led to high instances of account lockouts
- Led to ICT Service Desk being swamped with account reset requests
- Impacted the services provided by ICT

The Incident That Keeps on Giving

- Prior to event 28k authentification attempts every 3 day. During event 86k in 24 hours
- An attempt to authenticate every 1-3 seconds
- Service desk receiving 500 calls per day to unlock accounts (reminder – 4,000 users)
- 5 accounts trying to authenticate from overseas investigated

- This increase in activity happened each time incident was in the news (e.g. Amesbury)
- And when it wasn't in the news (e.g. anniversary of Salisbury)

The Incident That Keeps on Giving



Learning from continuation of incident (and not learnt)

- External events can impact your internal service
- Plan for them
  - We planned for physical disruption by protesters at a Council Meeting, but didn't plan for possible cyber disruption
  - But we are planning for National Armed Forces Day (being held in Salisbury
- Technical
  - Need to move to MFA or biometrics
  - Need to exploit O365 security more

Other Stuff

- Not all external communications are helpful
- Working at different security levels is “interesting”
- Authentification with NCSC can be lengthy
- Significant ICT work to support evacuation of Salisbury offices for decontamination (and to move back in)
- Engagement with NCSC provides a level of reassurance (NCSC on site visit)
- MHCLG also provided additional support

Summary of Impact

- Council/Police data was not compromised

BUT….

- It felt like a Denial of Service Attack
  - Service Desk stopped functioning
  - Works queues built up a backlog
  - 10%+ Council workers were locked out of their accounts on a daily basis
  - Mobile phones could not be used for email/calendar

Thank You

Stephen.Vercella@Wiltshire.gov.uk