February 2021: Area Wide Resilience Exercise

These notes are best viewed in conjunction with the slides from the above event, also available from Baker Street Quarter Partnership. This document forms a record of the participants' discussions of the questions posed and do not constitute professional advice or recommendations.

Escalating Scenario:
The Direct Action Cell has apparently committed its first act of protest.

- The incident occurred overnight close to the Baker Street area.
- Graffiti was extensively daubed on a building when it was closed and windows were smashed, causing damage estimated at several £000's
- There were no arrests.
- The Direct Action Cell focus is now clear.
- Your business is in the same sector but there is no direct threat against your premises or organisation.

In your Groups, please discuss the actions you would consider taking if any at this stage?

Some proportionate action to include consolidating building resilience, monitoring escalation and balance between sharing information with tenants and not overly worrying individuals at this stage.

Building Management:

- Minimise attendance outside of building – try and deter smokers / coffee breaks outside
- Hoarding company on standby
- Increase security provision to signal a 'not on my patch' message, including increasing presence outside of building, possible random security checks
- Monitor developing situation
- Notify clients and service partners
- Review current procedures.
- Message internal WhatsApp groups with key group, use internal PA system, send email to occupiers if overnight
- Consider access/egress: do all doors need to be open? Consider routes to office (public transport etc) for any disruption
- Sweep of local vicinity to remove potential implements (because MO was via smashed windows – remove eg scaffolding poles etc)
- Possible monitoring of open source information to supplement authoritative source information

Tenants/Businesses:

- Confirm with building management any procedures to be reviewed
- Senior staff members on standby/form decision making group

- Minimise attendance outside of building – try and deter smokers / coffee breaks outside
- Notify clients and service partners
- Review current procedures.
- Perhaps inform staff with balanced message: duty of care but not overly worrying – vs potentially instruct all staff to WFH or if critical in satellite office – no immediate threat but don't want to take chances

Police: conduct a Servator deployment for visibility , work with the safer neighbourhood team and investigate any commonalities with the building that was attacked.
Safer West End: Use of radios to supplement other channels of communication

Information Management and Remote Working

- You receive an email on your work email address purporting to be from the "Cell, " entitled "Just Introducing Ourselves."
- The message contains details relating to your business that would indicate knowledge only known to an employee (e.g. number of staff currently at work, procedure for opening up and closing the premises (if applicable), emergency assembly point, together with other specific financial/HR/operational details etc). There is no threat made to your business/premises.

Please consider the issues and the actions you think would be appropriate.

Discussions covered:
Investigation:

- Confirming how information had been compromised: insider threat or hacker? Check for lone wolf, contractors or third parties, staff should be using work laptops rather than their own? Is this blackmail or something else?
- Investigation: Cyber Security, Legal, HR: mobilise insider risk team
- Proportionate response based on whether one email or multiple emails received
- Given nature of the compromise (and depending upon the type of business), report the incident to the police and bring in "the experts" to help resolve the issue.
- Consider reporting to ICO breach of GDPR and Data Protection?
- Where was information found? Did they go through CEO's bins as they had found their home? Check domain for email – check outbound traffic – has something been sent by accident?

Consolidation:

- Consider enhancing overt security and the possibility of physical hostile reconnaissance
- Review and amend evacuation point
- Review personal information that may be online about staff
- Review company website and other open sources for any information breaches
- Remind staff of security policies

Recovery:

- How to share messages if corporate email and WhatsApp are not secure (if the system has been compromised)
- Possible increase in phone or face to face meetings (implications with remote working?)
- the need to keep critical information sharing regarding the breach to a tighter group (the CMT)
- One participating business has a Data Committee: this would be summoned to manage the impact.
- Consider MI6 training re insider threat – ensuring you are employing who you think you are

Crisis Response

- You are notified that 25 protestors have arrived outside the entrances/exits of your location.
- They have brought devices and some are "locked-on" to each other and are now barricading the front door(s) preventing staff from entering or leaving.
- You are advised that a member of your staff is amongst the protestors and he/she appears to be handing out sheets of paper to members of the public who have gathered to watch the demonstrators.

In your groups, please discuss your actions and the options you would consider.

Building management/facilities:

- Is it peaceful protest or not? This is key to determine response: is there a threat to staff or all likely to be over in a few hours?
- Communication with co-tenants of protestor's business
- Notify police and council
- Initiate lockdown procedures and emergency response plan instigated: focus on protecting our people and our assets
- Inability to leave building constitutes severe risk
- Security officer to use emergency button!
- Ensure CCTV is fully operational: use to monitor situation throughout building
- Ensure swipe access to floors above ground floor is operational: possibly lock internal doors until it's clear that the protest is only external
- Give response teams power to be agile and adaptable.

Businesses/Tenants (in multi-occupier building)

- If invacuation to another floor – try to do it floor by floor to enable social distancing
- need to preserve life in the face of an immediate threat took precedence over COVID requirements: suspend social distancing requirements. (comparison to recent Capitol attack in USA). Who would make this decision?
- The priority would be on the safety of colleagues and building initially, rather than the individual protester

- Advise other staff not to come to building and those in office to stay in (check all accounted for – what system to use?)
- Remind staff re media protocols and not commenting
- Involve HR in relation to protesting staff member

Comms

- Crisis team and comms to reassure: consider using different communication platforms to email
- If available, engage specialist PR/Comms to develop messages regarding the company position
- Remove the individual from teams comms or if concern insider job may go wider move to more manual calling trees

Engaging with the protestors directly was seen as potentially problematic: there may be a reputational risk and there was a view that the police should be left to sort things out
Some of the group would wish to engage directly with the member of staff involved in the protest. Others were content for the police to deal with any issues and follow up subsequently

Referenced Links and Further Reading:

CPNI Pandemic Security Behaviours Update - Nov 2020.pdf

CPNI Insider Threats in a Pandemic

NCSC Home Working: Preparing Your Organisation and Staff

NCSC Secure Home Working on Personal IT

How to check if any of your accounts might have been compromised
Have I Been Pwned

City of London Police Cyber Griffin Home Working Videos