ABERDEEN CITY COUNCIL

COMMITTEE	Audit & Risk Committee
DATE	23 February 2017
DIRECTOR	Richard Ellis, Interim Depute Chief Executive, Director of Corporate Governance
TITLE OF REPORT	Website Breach
REPORT NUMBER	CG/17/033
CHECKLIST COMPLETED	Yes/No

1. PURPOSE OF REPORT

This report is to update Elected Members of the website homepage breach on 28th January 2017.

2. RECOMMENDATION(S)

It is recommended that Elected Members note the contents of the report and attached appendices.

3. FINANCIAL IMPLICATIONS

As part of the investigation a third party was engaged to perform a vulnerability assessment of the website and associated infrastructure at a cost of £5,550.

The total cost of staff time (170 hours) involved with incident response and investigation to date is £4,540.

4. OTHER IMPLICATIONS

All implications detailed within the main body of this report.

5. BACKGROUND/MAIN ISSUES

The Incident

On the evening of Saturday the 28th January, the homepage of the Council's website was replaced with an external image. This occurred at 19.12 hours and normal web services were resumed to the public by

22.00 hours. Communications were issued to the public at 22.20 hours. Only the homepage was defaced, all other information on the website was still available and unaffected.

The Response

A full incident report is provided in Appendix A.

On Saturday 28th January 2017, an automatic alert was issued at 19.20 hours notifying IT of potential changes to the Council's website. At 20.20 hours the appropriate members of staff received notification. By 20.50 hours, an incident response team was established. At 21.11 hours the Head of IT & Transformation, the Interim Director of Corporate Governance and the Chief Executive were informed. The response team acted to restore the home page and prevent further intrusion. Messages were issued to the public via social media, the website and local media to reassure the public that no personal data was held on the site. There was no evidence that any data had been compromised or that the Council's main network had been breached.

There was significant press interest on the matter as the image displayed had connotations with ISIS. At this time there is no evidence to suggest whether this was the case. On Sunday 29th January the Head of IT & Transformation escalated the matter to the Chief Executive. The Chief Executive contacted Police and it was advised that this should constitute a formal investigation by Police Scotland. The incident team reconvened and a stay on external communications was initiated. A third party security firm was engaged to assist with vulnerability assessments.

On Monday the 30th January 2017 a formal investigation was launched by Police Scotland. It is anticipated that this investigation will take some time.

The incident response team continued to investigate the incident to identify the source of the hacking incident, to verify that no data had been breached and that any residual vulnerability had been identified. The incident team met daily with the Head of IT & Transformation, who in-turn reported updates to the Interim Director of Corporate Governance and the Chief Executive.

The Results

After initial investigation it is believed that the incident occurred due to a vulnerability found on the file upload facility on the 'What's On' page of the externally hosted internet website. It was also discovered that the hacking group were actively searching for UK Government websites with upload facilities at that time. This upload function has now been disabled. There is no evidence that any data was breached or that the Council's main network was compromised.

Actions

Actions arising are recorded within the Incident Report at Appendix 1.

6. **IMPACT**

Improving Customer Experience –

During the incident our customers experienced degradation to the Council's website. Customers were also unaware if their information was safe and protected as a result of the breach.

Improving Staff Experience –

Out of hours IT Support is currently on a voluntary standby rota through the RCC. There are no formal escalation processes for the on-call person for responding to major incidents. The nature of this incident highlighted that there is a requirement to review the call-out procedure and support for all staff across the council.

Improving our use of Resources –

As part of the Council's Being Digital Strategy a new website platform has been procured to replace the existing one. This will be delivered by the end of June 2017.

The current incident process has also been updated to take account of potential cybercrimes and an escalation process to Police Scotland is now in place.

Corporate –

The incident highlights the requirement for addressing all aspects of security when implementing Digital solutions. Systems hosted within the Council's network are protected through our Firewalls, Intrusion Protection, Anti-virus solutions, access control measures, both physical and electronic and environmental measures such as power protection, temperature and moisture monitoring and alerts. When procuring cloud based services, which are hosted external to the Council's perimeter network, systems are security assessed as part of the procurement process, and penetration tested to assure ourselves of the integrity of the Council's data prior to going live. Security system risk assessments are re-assessed annually.

Public –

Considering the social media activity around the website breach, this report is likely to be of interest to the public.

7. MANAGEMENT OF RISK

The main risks considered are reputation and trust in our core Council technology services, incorporating our protection of personal data.

Impact of a breach of the website is high as this forms part of the council's core critical business infrastructure. The likelihood of any of the council's public services, including the website, being attacked is a certainty. To mitigate this, various security measures are already in place with the aim to detect and block suspicious activity. Within our Being Digital strategy, the implementation of our replacement firewall solution is scheduled for March to June 2017. This firewall will enhance our network perimeter security to the latest technology. However, Cyber-criminals are continually devising new methods to avoid detection, and there is no guarantee that future breaches may not occur.

There is an added risk that many systems, which are not subject to the same vigorous security testing and change controls, have been procured and managed outside the central IT service. This is currently the subject of a review.

8. BACKGROUND PAPERS

None.

9. REPORT AUTHOR DETAILS

Paul Alexander, ICT Customer Services Manager, PAlexander@aberdeencity.gov.uk 01224 522606
Sandra Massey, IT Technology Services Manager, smassey@aberdeencity.gov.uk 01224 522778