Incident Report

This incident report provides a high level summary of events and actions taken to mitigate the issue. An additional incident report will be produced that will detail all technical actions taken.

Customer(s) affected:	Citizens / users of Aberdeen City Council public website		
Incident Start:	28/01/2017 @ 19:12	**Service Now incident ref:**	INC0023751
Incident Resolved:	28/01/2017 @ 22:00	**Duration:**	2 hours 47 minutes
		Priority:	P1
Affected Service(s) / Applications:	Aberdeen City Council website	**Service / Application Owner:**	ACC IT & Transformation

Summary of incident:

On the evening of Saturday the 28th January, the Aberdeen City Council website (www.aberdeencity.gov.uk) was hacked by an organisation called Team System DZ. The hacking took the form of an image covering the home page of the website.

Timeline of events:

28 January 2017

19:12: Aberdeen City Council Web files updated.
19:20: CERT UK monitoring alerted ACC ICT on call process.
20:11: Technology Team forwards alert on to Web Team to be raised with ACC web hosting vendor.
20:19: The hack is shared by citizens via the social media.
20:56: IT Technology Services Manager received initial alerts via text message from a member of IT & Transformation.
20:58: Incident escalated to Web Team by phone.
20:58: Customer Services Manager alerted by text from a member of his team.
21:00: IT Customer Services Manager notified by phone from a member of his team.
21:06: Text from Customer Services Manager to Interim Director Corporate Governance & Deputy Chief Executive, Head of IT and Transformation/SIRO and Head of HR & Customer Services asking them if they were aware of the incident.
21:10: IT Customer Services Manager notified Head of IT & transformation, Chief Executive and Interim Director Corporate Governance & Deputy Chief
21:15: IT Technology Services Manager confirmed with Technology Team that appropriate technical actions are initiated.
21:20: ACC Communications team notified.
21:21: Text from Customer Services Manager to comms Out Of Hours mobile advising of issue.
21:28: Customer Services Manager contacted RCC who had received no customer calls regarding the incident.
21:30: Web Team notified ACC website hosting company advising of a security breach.
21:40: Draft media response statement prepared.
22:00: ACC website site home page is fully restored. Initial analysis found the What's On feature on the home page was the most likely point of breach.
The approved statement was then issued on the Council's corporate social media accounts.
22:20: Infrastructure Architect arranged conference call between key stakeholders: Interim

Director Corporate Governance & Deputy Chief Executive Security Architect, IT Technology Services Manager, IT Customer Services Manager, Web Developer, Incident & Problem Co-ordinator, IT Support Co-ordinator, Communications Business Advisor, Customer Service Manager. Web developer provides update on analysis and findings so far, assured no personal data is held on the website.

22:30: Revised communication statement is approved and issued to the media, posted on social media platforms and on the front page of the website advising that no personal data is held on the website. 24 hour Regional Communication Centre staff advised to regularly monitor the website overnight.

29 January 2017

00:40: Web team emails analysis results and findings from the initial investigation.
06:34: RCC confirmed no customer calls received overnight.
10:00 – 18:00: Media Team managed enquiries from local and national press including: The Press and Journal, The Evening Express, Daily Mail, BBC North-East, BBC Scotland and The Scottish Sun.
16:06: Head of IT and Transformation informs Chief Executive of the hacking group's links to ISIS. Incident escalated by Chief Executive to Police Scotland Counter Terrorism Unit. A stay on all communications was instructed while the Police Investigation continues.
16:30: On site review convened at Marischal College with available stakeholders.
18:00: Conference call was held to follow up with web hosting vendor, who suggested that the hackers were able to breach the security of the site due to a weakness in the website itself rather than through their managed servers.
19:30: Security partner engaged to conduct scan of the web server.
21:00: Initial scan started by Security Partner.

Key findings, root cause and actions taken:

Initial analysis of the findings suggested that an exploit in the Aberdeen City Council website 'What's On/Events Online' feature allowed the hackers to upload a file via the image upload function. This allowed the hackers to move files to the root of the website, allowing the home page to be updated with the contents of the file. The 'What's On' component is used by members of the public to submit images associated with events. This feature of the website was subsequently disabled. Because the website is updated by ACC services using a devolved content management system, all content contributing was also disabled – this remains the case until the full investigation is concluded. At present the Aberdeen City Council website is therefore not being updated until the full conclusion of the investigation by both internal analysts and external security partners. Work is ongoing to establish a workaround for updating key content on the website.

IT & Transformation Technology Team conducted secure network perimeter checks in order to provide assurances to the business that no breaches had occurred within the core ACC network. This involved firewall, intrusion protection system checks, in depth scans of webservers and engagement with web hosting vendor to share server/traffic logs. Comprehensive anti-virus scans and monitoring has also implemented on any affected servers and databases.

IT & Transformation's security partner was initially engaged to conduct comprehensive cybersecurity testing for risks and vulnerabilities on the website and components of the internal infrastructure. An investigation as to the exact cause of the breach was conducted by the web team and all files and logs passed to our security partner for analysis. While root cause has been established, further security testing is ongoing. The resulting reports will be fully analysed with recommended actions arising from the report.

The suppliers of the content management system (application used to update content on the website) were engaged who checked the code within the application for any possible vulnerability. All checking was concluded successfully.

Details of the hack and the files in question were passed via secure USB drive to the Counter Terrorism Unit. The Local Authority Security Group and anti-virus providers were also advised of the incident.

No customer data is held within the Aberdeen City Council website infrastructure – any customer data is held within secure internal and third party systems. Therefore there is no evidence to suggest that the hackers managed to gain access to any component or database within the internal Aberdeen City Council network, or that any customer data was compromised.

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.

Caused by					
Application	**Software**	**Hardware**	**Network**	**Environmental**	**Other**
					Cybersecurity breach
Workaround:	N/A				

Contributory Causes			
Change / Service Request Related:	N/A	N/A	N/A

High Level Actions			
Action	**By (person/organisation)**	**Date**	**Status**
Security partners conducting further in depth analysis and granular penetration testing with a view to providing further risks and recommendations	Technology Team	03/02/2017	Closed
Continue in depth analysis of server / database files and logs	Web Team	03/02/2017	Closed and files sent to Police Investigation.
Establish workaround for content to be updated on the website	Web Team	03/02/2017	Closed – Web updated limited members of Web Team.
Review Out of Hours ICT call system	IT Team Leaders	10/02/2017	In progress – meeting arranged for week commencing 13th February
Change all server Administration passwords	Web Team	10/02/2017	Open

Provide information for security risk register	IT Technology Services Manager	10/02/2017	Closed
Upgrade and replace current content management system	PPR & Digital Engagement Manager	30/06/2017	In progress: New system has been procured as part of the Being Digital Strategy