North East Regional Organised Crime Unit website

Development of an accessible website for the North East Regional Organised Crime Unit (NEROCU) for the benefit of the community and the prevent, prepare and protect functions of the regional cyber crime unit.

First published
20 February 2025

Key details

Stage of practice	Untested
Purpose	Prevention
Topic	Community engagement Cybercrime Digital, data and analytics
HMICFRS report	**PEEL 2021/22: An inspection of the north-east regional response to serious and organised crime**
Contact	Paul Maddison
Email address	nerccuprotect@durham.police.uk
Region	North East
Partners	Police
Stage of implementation	The practice is implemented.

Key details

Start date	March 2021
Scale of initiative	Regional
Target group	Workforce

Aim

The aim for the creation of a North East Regional Organised Crime Unit (NEROCU) cyber website is to:

- create a central cyber information hub for the benefit of the community as well as the prevent, prepare and protect functions of the regional cyber crime unit
- reduce additional work created because of rapid content changes to products, services, threats, advice, and guidance for each force or the dedicated force hosting the content of the website
- ensure consistency of content across all platforms to avoid mixed messaging

Intended outcome

- Increase information flow for members of the Regional Cyber Crime Unit and the prevent, prepare and protect functions.
- Reduce workload for each force or dedicated force hosting content of the website.
- Improve content and clear messaging.

Description

During the building the of the website NEROCU:

- sought out and secured the services of a web developer to create the website
- had multiple planning meetings with web developer to lock in vision for website
- provided word press and accessibility courses for department staff who will have admin rights to website

Outdated website no longer fit for purpose. The old website contained old information and used plugins which were no longer supported. In cyber the need for current information is paramount in the ever changing and evolving cyber landscape. The old website could not host this in a way that would resonate with the target audience for cyber in the way the new website could do.

The website is managed by ROCU cyber staff with funding from existing budgets. £2,000 initial start-up cost and now recurring annual fees for hosting and website plugins. The implementation was a creative process which involved:

- procurement of the services of a web designer
- decision on content, layout, and corporate identity such as the colours, font and logos
- registration of a domain and purchase licences for all programmes required to run the website
- consultation with force legal teams
- consultation with the media team
- training of staff on website maintenance
- launching of the website.

The web team is made up of the web designer and ROCU cyber staff

Prior to the commencement of the project, the full support of the senior management team (SMT) was secured to enable the project to be signed off.

Overall impact

The website receives approximately 14,000 views per month. The website is used to publish vital vulnerability reports which are brought to the attention of regional managed service and cyber security providers who in turn will bring them to the attention of any affected customers.

Thousands of vulnerability reports have been made available to the service providers for the benefit of helping further secure their customers who are local business owners.

The website has been a useful source of information to the local service providers and business community. The cyber and business communities now receive current and relevant information on Cyber threats in the region where they did not before. For example, MSP Aspire Technologies report that the vulnerability reports they receive from the website are now part of their daily business.

The initiative achieved what it was set out to do as cyber communities and members of the public are better informed about the current and evolving cyber landscape.

Key metrics

- Q1 2024: 197 contacts to internet service providers (ISPs) covering 263 Known, 2709 critical, 5082 high, and 6102 medium vulnerabilities.
- Q2 2024: 179 contacts to ISPs covering 276 known, 3690 critical, 6570 high, and 6574 medium vulnerabilities.

Learning

A lot of lessons learned from the start of the process to the implementation.

The implementation was a creative process involving the procurement of expert resource, the design and layout of the website, registration, purchase of licences, consultation with the legal and media teams, the training of staff, getting the full support of the SMT, launch and ongoing maintenance of the site that now meets the needs of thousands of local service providers and businesses.

The website incurs annual reoccurring costs to maintain its running and presence online.

Copyright

Legal disclaimer

Tags

Community engagement Cybercrime