# Redcar and Cleveland Council cyber-attack reveals costly gaps in public sector security



In the early hours of February 8, 2020, a quiet alarm sounded at Redcar and Cleveland Council in north-east England, signalling a looming catastrophe. An IT engineer sped through wintery streets, responding to reports of a cyber-attack that would soon incapacitate the council's entire computer network, demanding urgent intervention to mitigate the damage. As Mary Lanigan, then leader of the council, recalled, the attack heralded a total collapse of their IT systems, plunging local services into chaos. "The destruction of our systems was total," she stated, a reflection of the crisis that would unfurl over the subsequent weeks.

The attack began with an unassuming email attachment, which, once opened, unleashed a malicious piece of software that lay dormant before wreaking havoc across the council's network. In a matter of hours, the malware thwarted staff access and scrambled critical files, leaving residents unable to access vital services such as waste collection or social support. The consequences were severe—vulnerable populations, including children supported by social services, were left without crucial assistance. Lanigan described the situation as “devastating,” not only for the council staff but importantly for the public who relied heavily on their services.

The cyber-attack highlighted a deeper issue. Ciaran Martin, the former head of the National Cyber Security Centre (NCSC), flagged the escalating threat of simultaneous attacks on public services, emphasising the potential for such incidents to "wreck lives." He termed the situation at Redcar as “unusually serious” given the implications for the well-being of children and vulnerable groups. Amidst this turmoil, the NCSC dispatched experts to assist the beleaguered council—a move that underscored the gravity of the crisis.

By February 10, council IT staff were scrambling to contain the fallout, resorting to manual processes to keep essential services afloat. Handwritten notes replaced digital records, and the council grappled with a severe backlog of service requests. One resident, Paul, found himself without the necessary support for his wife, Clare, whose health condition required regular care. "You'd be waiting on the phone for hours,” he recounted. The council’s shortcomings during this period only served to deepen the residents’ frustrations.

As the situation devolved, the consequences became clearer. Initial estimates of recovery costs ballooned, with projections reaching between £10 million and £18 million—figures that surpassed the council's annual budget. Such a staggering financial burden prompted the National Crime Agency to investigate the incident, revealing an extensive, high-stakes cyber-crime environment. Amidst a landscape of similar attacks on other public institutions, the need for heightened cybersecurity measures was more pressing than ever.

By the time the hackers made their ransom demands—rumoured to be in the low single digits of millions of US dollars—Lanigan had resolved against paying. "I’m a Yorkshire woman," she asserted, illustrating her determination not to capitulate to cyber criminals. Despite no formal ban against ransom payments at the time, the growing consensus in the UK government has shifted towards outlawing such arrangements in the public sector, a response to the increasing frequency and severity of ransomware attacks.

Although a temporary system was reinstated to restore some social services within weeks, full recovery proved to be a protracted affair, with the council only regaining about 90% of operational capability by May 2020. A meticulous rebuild of IT systems, some of which had to be constructed from scratch, extended the timeline for complete restoration to 10 months. Witness accounts from IT personnel underscored the extensive damage and the painstaking effort required to rectify it.

The unfolding narrative took another twist in 2022, when the spotlight turned to the Russian-based Conti Group, reportedly behind the attack. Following geopolitical turmoil, the group unraveled amid revelations from pro-Ukrainian hackers, exposing many notorious cyber criminals. This shift in the cyber threat landscape served as a reminder of the intricate web of international criminal activity that local councils like Redcar and Cleveland find themselves ensnared within.

As councils and public service entities grapple with the ramifications of such attacks, the incident at Redcar remains emblematic of the vulnerabilities faced by local authorities. The financial impact has been profound, with the UK government stepping in with significant grants to assist with recovery efforts. However, the reality is stark: as cyber-attacks grow increasingly sophisticated, so too must the strategies employed to defend against them. Public services hold the lives of communities in their balance, making their resilience not just a technological concern but a matter of social responsibility.

### Reference Map:

1. Paragraph 1: 1
2. Paragraph 2: 1
3. Paragraph 3: 1, 2
4. Paragraph 4: 1, 3
5. Paragraph 5: 1, 4, 6
6. Paragraph 6: 1
7. Paragraph 7: 1, 5
8. Paragraph 8: 1, 2, 3
9. Paragraph 9: 1, 4, 7
10. Paragraph 10: 1, 2, 3
11. Paragraph 11: 1, 2, 5
12. Paragraph 12: 1, 6, 7

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.bbc.com/news/articles/cpw72pxrgdzo> - Please view link - unable to able to access data
2. <https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack> - In February 2020, Redcar and Cleveland Borough Council in the UK suffered a significant cyber-attack that disabled its IT servers for three weeks. The attack led to the council's website and phone lines being inoperable, causing widespread disruption to public services. The council estimated the recovery costs to be between £11 million and £18 million, surpassing its annual budget. The National Crime Agency investigated the incident, and the council worked with the National Cyber Security Centre to restore services. Residents faced challenges accessing essential services during this period.
3. <https://www.bbc.com/news/uk-england-tees-52521769> - Following a ransomware attack in February 2020, Redcar and Cleveland Borough Council reported that 90% of its computer systems were operational by May 2020. The attack had rendered the council's website inoperable, and staff had to rely on pen and paper to maintain services. The National Crime Agency investigated the incident, and the council received assistance from the National Cyber Security Centre. Despite the challenges, the council continued to provide key services, including responses to the COVID-19 pandemic, during the recovery period.
4. <https://feeds.bbci.co.uk/news/uk-england-tees-57433800> - Redcar and Cleveland Borough Council initially estimated the cost of a cyber-attack in February 2020 at £10.4 million. However, after a financial impact assessment, the figure was revised to £8.7 million. The attack had disrupted online services for approximately 135,000 residents, leading to the use of manual processes. The council worked with the National Cyber Security Centre to restore services and enhance future security measures. The incident highlighted the growing sophistication of cyber-attacks targeting public sector organizations.
5. <https://www.cybercureme.com/redcar-and-cleveland-attack-recovery-cost-over-gbp10m/> - In August 2020, it was reported that the recovery costs for the cyber-attack on Redcar and Cleveland Borough Council in February 2020 exceeded £10 million. The attack had rendered online public services unavailable for over a week, affecting approximately 135,000 residents. The council's budget update report detailed costs for infrastructure recovery, system replacement, and impacts on council directorates. The incident underscored the financial and operational challenges posed by cyber-attacks on local government entities.
6. <https://www.thenorthernecho.co.uk/news/19217591.3-6m-grant-redcar-cleveland-council-hack/> - In April 2021, the UK government agreed to provide Redcar and Cleveland Borough Council with a £3.68 million grant to assist with the recovery costs from a ransomware attack in February 2020. The council had initially estimated the recovery costs at £10.4 million. The grant was intended to help cover the expenses incurred in rebuilding the council's IT systems and services. The incident had caused significant disruption to public services, and the grant aimed to support the council's efforts in restoring normal operations.
7. <https://www.localgov.co.uk/Redcar-receives-3.7m-towards-cost-of-cyber-attack/52151> - In April 2021, Redcar and Cleveland Borough Council received £3.7 million in 'exceptional financial support' from the UK government following a ransomware attack in February 2020. The grant was intended to cover recovery costs incurred over the past year. The council's total estimated cost for the cyber-attack was £10.4 million, encompassing impacts on council departments, reduced income, and repair or replacement of IT systems and equipment. The council had been working with the National Cyber Security Centre to strengthen its cyber defenses post-attack.