# Conti ransomware attack on Redcar council exposes severe local government vulnerabilities



In the early hours of 8 February 2020, an unsuspecting email with a seemingly harmless attachment became the catalyst for chaos within Redcar and Cleveland Borough Council's IT systems. This cyber-attack, attributed to the notorious Conti ransomware group, caught council officials unprepared and left essential public services in disarray. The attack raised significant alarms, not just locally but across the UK, highlighting the acute vulnerabilities of public institutions to cyber threats.

Mary Lanigan, then-leader of the council, recalled the devastation caused by the sudden attack. "I got a phone call to say: we've been hit," she explained. The consequences were immediate and severe, with the council’s digital operations rendered inoperable, impacting everything from bin collections to vital social services aimed at protecting the vulnerable. This incident is part of a broader narrative in which local councils have increasingly become targets for cybercriminals, a trend that has escalated remarkably over recent years.

In its wake, the attack brought to light stark issues concerning the adequacy of the UK's cyber infrastructure, particularly in local government. Ciaran Martin, the former head of the National Cyber Security Centre (NCSC), expressed that a simultaneous assault on multiple public services could be catastrophic, capable of "wrecking lives." Such fears seem justified considering the disruption at Redcar and Cleveland, which directly affected over 135,000 residents, many of whom were reliant on local services for health and welfare support.

As the situation unfolded, the council staff faced the daunting task of reverting to manual processes. The operational paralysis meant that even simple requests, such as bin collections, could not be addressed. "You had to be practical... it was actually getting more phones in there so that people could ring us," Lanigan noted, indicating the urgency and the chaos that gripped the council at that time. This shift to a manual mode, although necessary, demonstrated the fragility of local government operations dependent on technology.

For families like Paul and Clare, the situations were dire. Clare, who required ongoing assistance due to a debilitating condition, experienced significant delays in receiving support as functionally the council could barely operate. Their reliance on timely council communication turned into frustration as they waited “on the phone for hours,” with vital information being lost amid the transition back to paper and pen.

The financial implications of the attack were considerable. Initial estimates placed the recovery costs between £10 million and £18 million. These figures encapsulated a wide range of expenses from IT system repairs to losses from reduced income streams for services such as council tax and business rates. By May 2020, after intensive efforts, the council reported that around 90% of its systems were operational; however, it took nearly ten months for everything to be fully restored. IT worker Ben Saunders portrayed the recovery process as “very meticulous,” as much information had to be rebuilt from the ground up.

The attack spurred investigations led by the National Crime Agency, which underscored the sophistication involved in modern cyber threats. The council subsequently put enhanced security measures in place and sought specialist advice from the NCSC to guard against future incidents. The government stepped in with financial support, granting £3.68 million to assist in the recovery, but the council continued to grapple with the long-term impact of the incident.

With the cyber landscape constantly evolving, the government has considered stricter regulations regarding ransom payments by public sector bodies, suggesting a pivot towards a more proactive approach in preventing such attacks. However, at the time of the attack, Lanigan remained resolute in her stance: "There was no way I was paying any ransom to anybody."

The events that unfolded during and after the February 2020 attack serve as a stark reminder of the vulnerabilities faced by local councils in the digital age. They illustrate not only the need for enhanced protections and infrastructure but also the critical importance of public sector resilience in the face of escalating cyber threats. As the world grows increasingly reliant on technology, the harrowing experiences of Redcar and Cleveland Council inform a pressing discourse on cybersecurity, urging government and private sectors alike to take the necessary steps toward safeguarding vital public services.

### Reference Map

1. Paragraphs 1, 2, 3, 4, 5, 6, 7
2. Paragraph 6
3. Paragraphs 4, 5
4. Paragraphs 3, 5
5. Paragraphs 3
6. Paragraphs 3, 7
7. Paragraph 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.bbc.com/news/uk-england-tees-52521769> - In May 2020, Redcar and Cleveland Borough Council reported that 90% of its computer systems were operational again after a ransomware attack in February. The attack had rendered the council's website inoperable, forcing staff to use pen and paper to maintain services. The National Crime Agency investigated the incident, and the council emphasized the increasing sophistication of cyber-attacks. They also implemented enhanced security measures and received specialist advice from the National Cyber Security Centre during the recovery process.
3. <https://www.theguardian.com/technology/2020/feb/27/redcar-and-cleveland-council-hit-by-cyber-attack> - In February 2020, Redcar and Cleveland Borough Council suffered a cyber-attack that disabled its IT servers for three weeks, affecting its website and phone lines. The council estimated the recovery cost between £11 million and £18 million, surpassing its £7.4 million funding grant for 2020/2021. The National Crime Agency led the investigation, and the council acknowledged the attack as a 'ransomware cyber-attack' on 8 February. Despite the disruption, frontline services continued, and no personal information was reported as compromised.
4. <https://www.cybercureme.com/redcar-and-cleveland-attack-recovery-cost-over-gbp10m/> - A cyber-attack on Redcar & Cleveland Borough Council in February 2020 resulted in recovery costs exceeding £10 million. The attack caused online public services to be unavailable for over a week, affecting approximately 135,000 residents. The council's budget update report indicated that £2.4 million was spent on infrastructure and system recovery, £3.4 million on individual council directorates, and nearly £1 million due to reduced enforcement income and lower collection levels for council tax and business rates.
5. <https://feeds.bbci.co.uk/news/uk-england-tees-57433800> - Following a cyber-attack in February 2020, Redcar and Cleveland Council initially estimated the recovery cost at £10.4 million. However, after a financial impact assessment, the figure was revised to £8.7 million, citing lower-than-expected staffing and IT costs. The attack left about 135,000 residents without online access to public services, with staff resorting to using pen and paper. The National Cyber Security Centre assisted in restoring services, and the council received £3.68 million from the government to help rebuild its systems.
6. <https://www.localgov.co.uk/Redcar-receives-3.7m-towards-cost-of-cyber-attack/52151> - In April 2021, the UK government agreed to provide Redcar and Cleveland Borough Council with £3.7 million in 'exceptional financial support' following a ransomware attack in February 2020. The grant aimed to cover recovery costs incurred over the past year. The council's online services were disrupted during the attack, leading to the involvement of experts from the National Cyber Security Centre. The total cost to the council amounted to £10.4 million, including impacts on council departments and reduced income.
7. <https://www.thenorthernecho.co.uk/news/19217591.3-6m-grant-redcar-cleveland-council-hack/> - After a ransomware attack in February 2020, Redcar and Cleveland Borough Council received a £3.68 million government grant to help cover recovery costs. The council had initially estimated the incident's cost at £10.4 million. The attack disrupted all council services, including the website, and staff had to rely on pen and paper. The National Cyber Security Centre assisted in restoring the council's computer network, which now includes enhanced monitoring and intelligence of activity and threat.