# Redcar and Cleveland cyber-attack exposes critical vulnerabilities in public services



In February 2020, a cyber-attack on Redcar and Cleveland Borough Council plunged the local authority into chaos, illustrating the devastating potential of ransomware on public services. An email, innocuously disguised, contained malicious software that would soon lock staff out of critical systems, disrupting services across the board, from social care to waste collection. Mary Lanigan, at the time the council leader, recounted receiving a panicked call notifying her of the breach, stating that the "destruction of our systems was total." This incident was part of a broader trend, as public sectors globally face escalating cyber threats, with notable recent attacks on major retailers such as M&S and the Co-op.

Once the virus was triggered, the attack quickly incapacitated the council’s IT infrastructure, and by the morning of February 10, the digital landscape was unrecognisable, with staff resorting to pen and paper to manage operations. This regression not only hindered everyday tasks, such as addressing local concerns about bin collections, but also severely affected vital services aimed at protecting vulnerable populations. For example, Paul, a local resident, had to abandon his job to care for his wife after the attack disrupted the support services they relied on. His wife's condition, functional neurological disorder, necessitated timely assistance from care workers, which was compromised due to the crisis.

In an unusual move, the National Cyber Security Centre (NCSC) intervened due to the serious implications for public welfare, particularly regarding children’s safety. Ciaran Martin, who led the NCSC at the time, noted, “If a council is telling you they are worried about their ability to run services for vulnerable children, you take that very seriously.” The council was forced to call a Cobra meeting—a high-level government response to emergencies—to tackle the crisis, underscoring the attack's severity.

As recovery efforts unfolded, the financial implications began to emerge. The council initially estimated the costs of the recovery at approximately £10.4 million, a figure later adjusted to £8.7 million following a comprehensive financial assessment. Many critics deemed the £3.68 million government grant received to aid the recovery insufficient, highlighting concerns over transparency and the planning surrounding the council’s cyber-defences. This financial support was conditional, requiring external reviews of the council's financial stability and an ongoing assessment of its recovery processes.

Amidst the recovery, the community felt the ramifications acutely. With a population of around 135,000 residents, many struggled without access to online services. Recovery efforts were painstaking; IT workers described the process of rebuilding systems as meticulous and lengthy. By May 2020, the council reported that around 90% of its computer systems were operational. However, by then, significant gaps in data and service continuity had emerged; services such as social care were only partially restored, and many functions required rebuilding from scratch.

The attack drew attention to the rising threat to public services from sophisticated cyber criminals. Evidence from subsequent investigations indicated involvement from the Conti Group, a notorious ransomware gang that became fragmented following Russia's invasion of Ukraine. This event exposed a network of cyber criminals whose operations extended far beyond small-scale local attacks, revealing a concerning trend that links cybersecurity threats to geopolitical issues.

As public and private sectors grapple with the ascending tide of cyber threats, the case of Redcar and Cleveland serves as a potent reminder of the vulnerabilities inherent in our digital dependencies. The pressing challenge now is ensuring robust defences to protect public infrastructure and maintain essential services for the communities that rely on them.

The ramifications of the Redcar and Cleveland attack continue to resonate, prompting discussions about the future of cyber-security policy, particularly regarding government guidelines about ransom payments. With experts calling for more stringent regulations, the urgency for enhanced protective measures remains paramount.

### Reference Map

1. Article on the cyber-attack at Redcar and Cleveland Council.
2. Details on recovery timelines and costs.
3. Government grant implications and community impact.
4. Discussion on the involvement of the Conti Group and rising cyber threats.

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, far exceeding its annual budget. The National Crime Agency investigated the incident, and the council received a £3.68 million government grant to aid in rebuilding its systems. The attack highlighted the increasing sophistication of cyber threats targeting public services.
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 again by May 2020. The attack had initially rendered the council's website inoperable and forced staff to rely on pen and paper to maintain services. The council worked with the National Cyber Security Centre to rebuild its systems with enhanced security measures. Despite the progress, the council did not disclose the total cost of restoring and rebuilding its IT infrastructure.
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 down to £8.7 million. The attack had left approximately 135,000 residents without access to online public services, and staff had to revert to using pen and paper. The council received a £3.68 million government grant to assist with the recovery, though critics argued it was insufficient compared to the initial estimates.
5. <https://www.cybercureme.com/redcar-and-cleveland-attack-recovery-cost-over-gbp10m/> - A cyber-attack on Redcar and 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 estimated that £2.4 million was spent on infrastructure and system recovery, £3.4 million on costs to individual council directorates, and nearly £1 million due to reduced enforcement income and lower collection levels for council tax and business rates. The council has since worked to enhance its cyber-defenses and is enrolled in a National Cyber Security Centre scheme.
6. <https://www.thenorthernecho.co.uk/news/19217591.3-6m-grant-redcar-cleveland-council-hack/> - In response to a ransomware attack in February 2020, Redcar and Cleveland Borough Council received a £3.68 million government grant to aid in rebuilding its IT systems. The attack had caused significant disruption, with the council's website and online services being inoperable for weeks. The council initially estimated the recovery costs at £10.4 million, but this was later revised to £8.7 million. The grant was intended to help cover the costs incurred in the past 12 months, with conditions including an external assurance review of the council's financial position.
7. <https://www.localgov.co.uk/Redcar-receives-3.7m-towards-cost-of-cyber-attack/52151> - The UK government provided Redcar and Cleveland Borough Council with £3.7 million in 'exceptional financial support' following a ransomware attack in February 2020. The total cost of the attack was estimated at £10.4 million, covering impacts on council departments, reduced income, and repair or replacement of IT systems. The grant was intended to cover recovery costs incurred over the past 12 months, with conditions including an external assurance review of the council's financial position and an independent assessment of the council's recovery work and current cyber resilience.