RiskSpotlight

# Scenario: Ransomware Attack on RWS Group's Retail Banking CRM System

# Table of Contents

**Scenario Title:** Ransomware Attack on RWS Group's Retail Banking CRM System

## Scenario Overview

In early 2024, RWS Group, a prominent financial institution in the UK, fell victim to a severe ransomware attack targeting its retail banking division. Orchestrated by the notorious cybercriminal group known as the "BlackCat Syndicate," the attack exploited vulnerabilities in the retail division's customer relationship management (CRM) software, which had not been updated following recent system upgrades. The infiltration led to the deployment of a malicious ransomware called "LockSafe", paralysing critical customer transaction processing systems, compromising sensitive client data, and disrupting internal communications across the bank's extensive network.

The immediate aftermath of the attack saw the BlackCat Syndicate demanding a ransom of £5 million in cryptocurrency, with threats of releasing the stolen sensitive data and permanently encrypting the bank's critical files. RWS Group, prioritising the restoration of its critical operations and safeguarding customer information, complied with the demand, paying the hefty sum within the stipulated 72-hour deadline. This incident not only resulted in substantial financial losses but also severely impacted the bank's operational integrity, customer trust, and market reputation, prompting a comprehensive review of security protocols and crisis management strategies within the institution.

## Scenario Background

| | |
|---|---|
| **Initial IT Modernisation Programme Launch** | RWS Group initiated a five-year IT modernisation programme aimed at overhauling its legacy systems. The focus was to transition all operational IT frameworks to cloud services provided by Microsoft Azure and Amazon AWS. Two years into the program, significant parts of the infrastructure were successfully upgraded, but some critical systems, including the retail banking CRM software, were still pending updates. |
| **Vulnerability Assessment Oversight:** | During the transition, a routine vulnerability assessment intended to be conducted post-upgrade was overlooked for the CRM system used in retail banking. This system, critical for customer data management and transaction processing, remained on the older security protocol, missing crucial security patches |
| **Staff Training and Resource Allocation** | In the lead-up to the attack, the IT department faced challenges due to resource allocation. With a significant portion of the IT staff based in offshore locations in Krakow and Mumbai, and others preoccupied with the modernisation efforts, regular updates and training on new security practices were delayed. |
| **External Security Audit Postponed** | An external audit scheduled to assess the security integrity of the newly implemented systems was postponed due to conflicting schedules with the modernisation rollout. This audit was also supposed to include a review of the yet-to-be-updated systems. |
| **Increased Cyber Threat Intelligence Reports** | In the months leading up to the attack, RWS Group's cybersecurity team noted an increase in threat activity reports, specifically targeting financial institutions by Eastern European cybercrime syndicates. Despite this, specific actionable intelligence on the BlackCat Syndicate was not effectively communicated to the operational teams. |
| **Software Upgrade Delays** | The CRM software's upgrade was delayed multiple times due to compatibility issues with other interfacing systems that were already upgraded. This created a mismatch in the security levels across the systems, leaving exploitable gaps. |
| **Lack of Emergency Preparedness Drills** | Prior to the ransomware attack, RWS Group had not conducted any emergency preparedness drills for a ransomware scenario within the last fiscal year, leaving staff unfamiliar with immediate response protocols in such an event. |
| **Insufficient Incident Response Team Readiness** | The internal incident response team, while established, was not fully prepared for an attack of this scale. Their last training on ransomware-specific scenarios was conducted over a year ago, focusing primarily on theoretical rather than practical, hands-on response strategies. |

| | |
|---|---|
| **Regulatory Compliance Pressures** | Amidst navigating compliance with newly introduced financial regulations in multiple operational regions, the bank's focus on regulatory adherence partially overshadowed the urgency needed for IT security enhancements, particularly concerning customer data protection. |

These events and oversights collectively formed a precarious foundation, inadvertently facilitating the eventual cybersecurity breach that had severe repercussions for RWS Group.

## Phase 1: Initial Detection and Response

In late February 2024, the early signs of the ransomware attack began to manifest subtly within the RWS Group's retail banking division.

- **February 20, 2024, 08:30 AM GMT**: The day started with a minor glitch reported in the CRM system's transaction processing module. The issue was initially logged by a customer service representative in London after several customers reported delays in transaction processing. The IT support team, based primarily in Manchester, noted the complaint but considered it a low-priority issue, typical of post-upgrade teething problems.
- **February 21, 2024, 11:45 AM GMT**: The following day, the frequency of similar reports increased. Complaints came not only from London but also from branches in Birmingham and Manchester. By midday, approximately 200 transaction delay incidents were logged, affecting around 400 customers. Each affected transaction showed an unusual processing time of up to 5 minutes, significantly higher than the standard few seconds.
- **Stakeholders Impacted**: The initial glitches impacted retail banking customers, particularly those trying to conduct time-sensitive transactions. Internally, customer service representatives and branch managers began expressing their concerns, noting an increase in customer dissatisfaction and operational disruptions.
- **February 22, 2024, 02:30 PM GMT**: The Retail Banking Risk Management Committee convened an emergency meeting to discuss the escalating number of incident reports. The committee decided to elevate the issue to the IT Security Team for a detailed investigation, suspecting a potential security breach rather than a simple software malfunction.
- **February 23, 2024, 09:00 AM GMT**: The IT Security Team initiated a forensic analysis and discovered anomalous code executions within the CRM software's backend, which were not part of the recent updates. This raised alarms about a possible cybersecurity incident. The team immediately implemented increased monitoring across all network traffic and escalated the issue to the Group's Chief Information Security Officer (CISO).
- **February 24, 2024, 07:00 PM GMT**: By the evening, the IT Security Team observed a spike in outbound traffic from the CRM system's servers to several IP addresses located in Russia, indicative of data exfiltration. This confirmed that the retail banking division was under a targeted attack, likely orchestrated to infiltrate deeper into the bank's network.
- **Internal Response**: The CISO promptly informed the executive management and activated the bank's initial cyber incident response protocol. This included isolating the affected systems, enhancing firewall protections, and increasing scrutiny of all network traffic. The communications department was tasked with preparing to manage any fallout by drafting preliminary statements to stakeholders, outlining that an investigation was underway and reassuring them of the bank's commitment to security.
- **February 25, 2024, 10:15 AM GMT**: The first concrete evidence of ransomware, identified as "LockSafe", was found encrypted on a server hosting client transaction data. The IT Security Team managed to trace the ransomware's entry point back to the unpatched vulnerabilities in the CRM software.

This phase of the scenario, marked by initial disruptions and swift internal responses, showcased RWS Group’s attempt to manage the unfolding crisis with increasing urgency, although the full magnitude of the breach was yet to be realised. The bank's retail customers and internal operational teams felt the immediate impact, prompting a series of rapid engagements and decisions aimed at mitigating the early stages of what was shaping up to be a severe security incident.

# RiskSpotlight

Forward-looking risk management

**For more scenarios & other forward-looking content try the Portal free for 2 weeks, no cost or obligation at https://www.riskspotlight.com/riskspotlight-portal/**


**RiskSpotlight Limited**

1st Floor, Radius House, 51 Clarendon Rd, Watford WD17 1HP, UK

portalsupport@riskspotlight.com

www.riskspotlight.com

@riskspotlight