Analysis of the Hampton Roads Sanitation District Ransomware Attack of November 2020

I. Executive Summary

In November 2020, the Hampton Roads Sanitation District (HRSD), a critical wastewater treatment utility serving a large population in eastern Virginia, experienced a significant ransomware attack. The attack involved the Ryuk ransomware, preceded by an initial infection with ZLoader malware. This cyber incident led to the shutdown of several HRSD business information systems, most notably impacting customer-facing services and billing operations. Despite these disruptions, HRSD successfully maintained the full operational status of its wastewater treatment services, ensuring continued compliance with all regulatory requirements. The organization immediately initiated a robust response, which included the shutdown of affected systems and the engagement of external cybersecurity experts. HRSD also proactively addressed the impact on its customers by offering alternative bill payment methods and assuring them of no late fees during the disruption. While the investigation into the attack's cause remained ongoing at the time of the initial public disclosure, HRSD demonstrated a commitment to transparency through consistent communication. Notably, the recovery process was relatively swift, with HRSD restoring most business operations within approximately three weeks, a feat largely attributed to their cyber insurance policy. This incident serves as a critical learning opportunity for organizations within critical infrastructure sectors, underscoring the persistent threat of ransomware and the importance of proactive cybersecurity measures and effective incident response strategies.

II. Introduction

The Hampton Roads Sanitation District (HRSD) plays a vital role in protecting public health and the environment in eastern Virginia by providing wastewater treatment services to approximately 1.7 million people across 20 cities and counties.[1] Given its crucial function in maintaining sanitation and environmental integrity, the security and resilience of HRSD's operations are paramount. On November 19, 2020, HRSD issued a news release to inform the public about a significant cybersecurity incident: a ransomware attack that had affected some of its computer systems.[2] The primary purpose of this initial communication was to acknowledge the attack and provide preliminary details regarding its impact and the organization's response. Key points highlighted in the release included the fact that a ransomware attack had occurred,

the specific business systems that were disrupted, the continued operation of essential wastewater treatment services, the immediate response and engagement of cybersecurity experts, the temporary impact on customer services (particularly bill payments), and the ongoing nature of the investigation. This report aims to provide a comprehensive analysis of the HRSD ransomware attack, drawing upon publicly available information, including the initial news release and subsequent reports, to detail the timeline of events, the scope of the impact, HRSD's response and recovery efforts, and the lessons that can be learned from this incident. The objectives are to offer a thorough understanding of the attack and its ramifications, particularly for organizations operating within critical infrastructure sectors.

III. Detailed Account of the Ransomware Attack

The ransomware attack on HRSD unfolded in the latter half of November 2020, with the initial detection occurring on the evening of Tuesday, November 17, 2020.[1] However, forensic analysis later revealed that the initial stages of the attack occurred much earlier. Evidence indicated that threat actor activity had commenced as early as October 23, 2020, with the introduction of ZLoader malware into HRSD's environment.[9] This nearly month-long period between the initial compromise and the eventual deployment of ransomware highlights the potential for attackers to remain undetected within a network, allowing them to conduct reconnaissance, escalate privileges, and identify critical systems before launching their primary attack.[9] The Ryuk ransomware itself was ultimately executed on the HRSD network around November 18, 2020.[9]

Upon learning of the ransomware attack, HRSD initiated immediate response efforts aimed at containing the intrusion.[2] This included the necessary step of shutting down some of its business information systems.[2] Recognizing the severity of the situation, HRSD's Chief Information Security Officer (CISO), Roger Caslow, made the decisive call to order a hard disconnect of systems. This proactive measure of physically disconnecting systems, including servers and internet connections, was crucial in preventing the ransomware from spreading further throughout the network.[1] Such immediate and decisive action underscores the importance of a well-defined and practiced incident response plan.

The ransomware attack directly impacted several of HRSD's key business information systems. These included HRSD business email accounts, the HRSD Customer Call Center, the Customer Self-Service portal, iSupplier web functionality (used for vendor interactions), and iRecruitment web functionality (used for recruitment processes).[2]

Notably, the attack also affected the billing system, leading to a suspension of billing operations.[1] The impact extended to HRSD's internal infrastructure, with many Windows computers being affected [1], and accounting and billing operations coming to a halt.[9] For a period, HRSD's phone and computer systems were entirely offline and inaccessible.[4] The targeting of these specific systems, particularly those related to business operations and customer interaction, suggests that the attackers aimed to disrupt HRSD's ability to function effectively and to exert pressure for a ransom payment. The widespread nature of the impact underscores the effectiveness of the Ryuk ransomware in penetrating and encrypting systems within HRSD's IT environment.

IV. HRSD's Immediate Response and Recovery Efforts

In the immediate aftermath of the ransomware attack, HRSD undertook several crucial actions to contain the damage and initiate the recovery process. As previously mentioned, the shutdown of affected business information systems was a primary step.[2] Further containment measures included the physical disconnection of all internet connections to prevent any further communication with external threat actors.[9] As a precautionary step, HRSD also disconnected its Linux-based systems.[9] These swift and decisive actions demonstrate a proactive and well-rehearsed incident response protocol, essential for limiting the propagation of ransomware across a network.

Recognizing the complexity and severity of the attack, HRSD promptly engaged the assistance of external cybersecurity experts.[2] These specialists worked continuously to restore HRSD's compromised business operation systems.[2] While the initial news releases did not specify the names of these experts [3], later information revealed that HRSD collaborated with cybersecurity consultants.[4] A significant factor in HRSD's recovery was its cyber insurance policy, which played a crucial role in facilitating the engagement of specialized firms. Specifically, CrowdStrike was brought in for incident response, and Moxfive was tasked with the rebuilding of the affected systems.[1] This highlights the strategic importance of cyber insurance not just for financial coverage but also for access to specialized expertise that can significantly expedite the recovery process from a sophisticated ransomware attack. In addition to external support, HRSD's internal IT professionals also played a vital role in the recovery efforts.[4]

The recovery process for the affected systems unfolded over several weeks. The initial news on November 19, 2020, indicated ongoing restoration work.[2] By December 1, 2020, while efforts to restore business systems safely were still underway, the billing system remained suspended, and customer account balances were not being

updated.[4] On December 16, 2020, HRSD's General Manager, Tim Henefin, reported that the organization was beginning the process of catching up on the backlog of payments and bills.[5] The billing system was ultimately restored in December 2020.[13] According to the BankInfoSecurity podcast, HRSD achieved a significant level of recovery, getting back on its feet, in approximately three weeks following the attack.[1] By January 6, 2021, all bill payment and customer contact methods had been fully restored.[13] The efforts of the IT Department in the restoration process were formally recognized in November 2021 with a commendation resolution.[31] The relatively swift recovery timeline suggests a commendable level of preparedness and effective execution of their incident response plan, significantly aided by the expertise brought in through their cyber insurance.

V. Ensuring Operational Continuity of Wastewater Treatment Services

A critical aspect of HRSD's response to the ransomware attack was its ability to maintain the continuity of its essential wastewater treatment services. Throughout the incident, HRSD consistently affirmed that all wastewater treatment services and processes remained fully operational.[1] This was largely attributed to the effective segregation between HRSD's operational technology (OT) systems, which control the physical wastewater treatment processes, and its information technology (IT) environment, which supports business operations.[1] This network segmentation proved to be a crucial security control, preventing the ransomware from impacting the core function of the utility. General Manager Tim Henefin further reassured the public that sewer service was never interrupted and that the treatment processes continued without any issues.[5]

Furthermore, HRSD consistently maintained compliance with all relevant regulatory requirements throughout the cyberattack.[2] This demonstrates the resilience of their core operations and their commitment to adhering to environmental and public health standards even during a significant cyber disruption. The ability to continue meeting these requirements is vital for maintaining public trust and avoiding potential regulatory penalties.

VI. Impact on HRSD Customers

The ransomware attack did result in several disruptions to services directly affecting HRSD customers. Notably, access to HRSD business email accounts was disrupted, hindering a common communication channel.[2] The HRSD Customer Call Center was also temporarily shut down, preventing customers from contacting HRSD via phone for

inquiries or support, although an alternative number for bill payments was later provided.[2] The Customer Self-Service portal, a key tool for customers to manage their accounts online, was also unavailable.[2] Additionally, the iSupplier and iRecruitment web functionalities, while not directly customer-facing, were also impacted, affecting vendors and potential employees.[2] A significant impact on customers was the temporary unavailability of in-person bill payments.[2] Furthermore, the billing process across the entire service region faced disruption for several weeks, affecting November and December bills and customers' ability to access their account information.[14]

To mitigate the impact on bill payments, HRSD offered alternative methods to its customers. These included the ability to make payments by phone by calling 844-257-6063 and online through a provided link.[2] Additionally, HRSD made provisions for customers wishing to pay their bills in person with cash by offering this option on weekdays at their facility in Virginia Beach.[4] Recognizing the inconvenience caused by the disruptions, HRSD assured its customers that no late fees or interest would be applied to payments delayed during this period.[2]

To address customer inquiries and provide support during the outage, HRSD established a dedicated phone line for bill payments and later for general inquiries.[2] An email address was also provided for urgent billing-related questions.[4] Following the restoration of the billing system, HRSD increased its call center staff to manage the anticipated surge in customer concerns.[13] Customers were advised to expect longer than usual wait times when contacting the call center due to the high volume of inquiries.[13]

VII. Investigation into the Cause of the Ransomware Attack

At the time of the initial news release and in subsequent communications, HRSD consistently stated that the investigation into the precise cause of the ransomware attack was ongoing.[2] As of December 16, 2020, HRSD General Manager Tim Henefin noted that the search for the perpetrators was still underway, and the organization was awaiting the results of the ongoing investigation and forensic analysis.[5]

Publicly available information has shed some light on the nature of the attack. The ransomware involved was identified as Ryuk.[1] Ryuk is known to be a ransomware-as-a-service (RaaS) group, where developers provide the ransomware to other cybercriminals who then execute attacks and share a portion of the ransom.[1] This particular ransomware has been associated with significant financial gains for its

operators and has frequently targeted critical infrastructure organizations, including those in the water and wastewater sector.[1] The initial point of entry for the attack appears to have involved ZLoader malware.[1] Forensic analysis indicated that the ZLoader infection likely occurred through a malicious Excel spreadsheet that was opened by an end user.[1] This multi-stage attack, beginning with ZLoader and culminating in the deployment of Ryuk, suggests a sophisticated and persistent threat actor. Additionally, the attackers utilized Cobalt Strike, a commercial red team software, for command and control within HRSD's network.[9] The presence of Cobalt Strike signifies that the attackers had established a significant foothold within the environment and were actively managing their malicious activities.

VIII. Analysis of HRSD's Public Communication Strategy

HRSD's public communication strategy in response to the ransomware attack appears to have been well-executed and effective. The initial news release, issued promptly on November 19, 2020, served as a timely notification to the public.[2] The title itself, "HRSD Computer Systems Struck by Ransomware Attack," was direct and transparent.[2] By providing specific details about the business systems that were affected, HRSD allowed its customers to understand the potential impact on their interactions with the utility.[2] Crucially, HRSD immediately reassured the public that its core wastewater treatment services remained operational, directly addressing a primary concern for a utility provider.[1] The communication also outlined the immediate response efforts undertaken, including the shutdown of affected systems and the engagement of cybersecurity experts, demonstrating that HRSD was taking the incident seriously.[2]

Recognizing the disruption to bill payments, HRSD proactively provided clear guidance on alternative payment methods, thereby mitigating potential inconvenience for its customers.[2] The assurance that no late fees or interest would be charged on delayed payments further demonstrated a customer-centric approach.[2] HRSD also committed to providing updates on the ongoing investigation and the progress of system restoration.[2] Subsequent news releases provided updates specifically on the suspension and eventual restoration of the billing system.[4] Additionally, FAQs provided by the City of Norfolk offered further clarification and addressed potential public concerns.[16]

HRSD's initial communication included an apology for the inconvenience caused by the attack [2], and the Director of Finance, Jay Bernas, also specifically apologized for the billing issues.[13] To facilitate media inquiries and ensure a point of contact for further

information, HRSD clearly provided the contact details for its Director of Communications, Leila Rice, in the news releases.[3] Overall, HRSD's public communication strategy appears to have been effective in providing timely, accurate, and reassuring information to the public during a challenging situation.

IX. Cybersecurity Measures and Recommendations

The ransomware attack on HRSD provides several insights into the organization's cybersecurity posture and offers valuable lessons for other entities. While HRSD's General Manager acknowledged the constant challenge of staying ahead of cyber threats despite having a sophisticated IT department [5], the initial infection through a phishing attack highlights the persistent vulnerability posed by human error.[1] The extended dwell time of the attackers within HRSD's network, nearly a month between the initial ZLoader infection and the Ryuk ransomware deployment, suggests potential areas for improvement in threat detection and monitoring capabilities.[9] A significant strength in HRSD's defense was the fact that its operational technology (OT) systems remained unaffected, indicating a robust level of network segmentation between the OT and IT environments.[1] HRSD's immediate engagement of cybersecurity experts and its utilization of cyber insurance demonstrate a proactive approach to incident response and recovery.[1] The subsequent adoption of enhanced email protection measures [36] indicates a commitment to learning from the incident and strengthening defenses. Furthermore, HRSD was already in the process of improving its information security practices prior to the attack, suggesting an ongoing awareness of the cyber threat landscape.[1]

Based on the HRSD experience and general best practices in cybersecurity, several recommendations can be made for organizations seeking to strengthen their defenses and improve their incident response capabilities:

- **Enhance Email Security:** Implement advanced email security solutions that go beyond basic spam filtering to include robust anti-phishing capabilities and behavioral analysis. Regularly conduct employee training and awareness programs focused on identifying and reporting suspicious emails, as phishing remains a common entry point for ransomware.[36]
- **Strengthen Detection Capabilities:** Invest in and continuously refine threat detection and monitoring tools and processes. This includes implementing endpoint detection and response (EDR) solutions and security information and event management (SIEM) systems to identify and analyze suspicious activities within the network in a timely manner. Reducing attacker dwell time is crucial.[41]

- **Regular Security Assessments and Penetration Testing:** Conduct periodic comprehensive security assessments and penetration testing of both IT and OT environments. These exercises can help identify vulnerabilities and weaknesses that could be exploited by attackers.[45]
- **Review and Update Incident Response Plan:** Ensure that a comprehensive incident response plan is in place, regularly reviewed, updated based on evolving threats, and tested through realistic tabletop exercises. All relevant teams should be familiar with their roles and responsibilities in the event of a cyber incident.[41]
- **Reinforce Network Segmentation:** Maintain strict network segmentation, particularly between OT and IT networks, and regularly audit these controls to prevent the lateral movement of attackers and the spread of malware to critical operational systems.[1]
- **Implement Multi-Factor Authentication (MFA):** Enforce the use of multi-factor authentication for all critical systems, accounts, and remote access points to add an extra layer of security and reduce the risk of unauthorized access due to compromised credentials.[42]
- **Maintain Robust Backup and Recovery Systems:** Implement a comprehensive backup strategy that includes regular backups of critical data and systems, storing backups offline and in a secure location. Regularly test the backup and recovery processes to ensure data can be restored quickly and efficiently in the event of a ransomware attack or other disaster.[9]
- **Develop a Comprehensive Communication Plan:** Establish a clear and well-defined communication plan for both internal and external stakeholders to be activated in the event of a cyber incident. This plan should outline who needs to be informed, what information should be shared, and the channels of communication to be used.[41]
- **Consider Cyber Insurance:** Maintain adequate cyber insurance coverage that includes not only financial reimbursement for losses but also access to experienced incident response teams and other specialized services that can be crucial for a swift and effective recovery.[1]
- **Information Sharing:** Actively participate in industry-specific information sharing and analysis centers (ISACs) and other relevant forums to stay informed about the latest threats, vulnerabilities, and best practices in cybersecurity.[35]

X. Conclusion

The ransomware attack on the Hampton Roads Sanitation District in November 2020 serves as a stark reminder of the persistent and evolving cyber threats facing critical

infrastructure organizations. The incident highlights the potential for significant disruption to business operations and customer-facing services. However, HRSD's response demonstrates the importance of preparedness, swift action, and effective communication. The successful maintenance of essential wastewater treatment services due to network segmentation underscores the critical role of this security control in protecting OT environments. HRSD's transparency in communicating with its customers and providing alternative solutions helped to mitigate the negative impact of the service disruptions. The lessons learned from this incident are invaluable for other organizations in critical infrastructure sectors. The need for continuous vigilance, proactive cybersecurity measures, and well-tested incident response plans remains paramount in safeguarding essential services and protecting public health and safety in the face of increasingly sophisticated cyber threats.

Key Tables:

Table 1: Timeline of the HRSD Ransomware Attack

Date/Time	Event Description
October 23, 2020	Initial ZLoader malware activity detected [9]
November 17, 2020	Cobalt Strike beacon creation [9]
November 18, 2020	Ryuk ransomware deployment (approximate) [9]
November 19, 2020	HRSD issues initial news release about the attack [2]
December 2020	HRSD billing system restored [13]
January 6, 2021	All bill payment and customer contact methods restored [13]

Table 2: Impacted Business Information Systems

System Name	Description/Impact
HRSD business email accounts	Communication disruption [2]
HRSD Customer Call Center	Communication disruption [2]
Customer Self-Service portal	Service unavailability [2]
iSupplier web functionality	Vendor interaction disruption [2]
iRecruitment web functionality	Recruitment process disruption [2]
Billing system	Payment processing disruption [1]

Table 3: Alternative Bill Payment Methods Offered

Payment Method	Details
Phone payment	Call 844-257-6063 [2]
Online payment	Link provided (http://www.invoicecloud.com/hrsd-hrubs) [2]
In-person cash payment	1434 Air Rail Avenue, Virginia Beach, VA (Weekdays, 8:00 a.m. - 4:30 p.m.) [4]

Works cited

1. The Ransomware Files, Episode 3: Critical Infrastructure, accessed April 29, 2025, https://www.bankinfosecurity.com/interviews/ransomware-files-episode-3-critical-infrastructure-i-4993
2. HRSD, accessed April 29, 2025, https://www.hrsd.com/node?page=86
3. News Release - November 19, 2020 | HRSD, accessed April 29, 2025, https://www.hrsd.com/news-release-november-19-2020
4. News Release - December 1, 2020 | HRSD, accessed April 29, 2025, https://www.hrsd.com/news-release-december-1-2020
5. HRSD continues to recover from cyber attack | 13newsnow.com, accessed April 29, 2025, https://www.13newsnow.com/article/money/hrsd-recovers-from-cyber-attack/291-0aeb2f81-137a-4869-9c2e-63493e3e4a4a
6. News Release - December 1, 2020 - HRSD, accessed April 29, 2025, http://www.hrsd.com/news-release-december-1-2020
7. Ransomware attack on Hampton Roads Sanitation District knocks out billing system, accessed April 29, 2025, https://databreaches.net/2020/12/02/ransomware-attack-on-hampton-roads-sanitation-district-knocks-out-billing-system/
8. Clippings - HRSD, accessed April 29, 2025, https://www.hrsd.com/clippings
9. des.sc.gov, accessed April 29, 2025, https://des.sc.gov/sites/scdph/files/media/document/BOW_Cybersecurity_HRSDRoundTableDiscussion.pdf
10. HRUBS Billing Remains Suspended - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicSend/ViewMessage/message/130488
11. HRSD continues to recover from cyber attack, accessed April 29, 2025, https://www.nacwa.org/news-publications/news-detail/2020/12/16/hrsd-continues-to-recover-from-cyber-attack
12. HRUBS Statements Delayed due to November 2020 ... - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicAlerts.asp?AID=5215&ARC=10297
13. HRSD: Utility payment due dates extended for November, December bills | 13newsnow.com, accessed April 29, 2025, https://www.13newsnow.com/article/news/local/mycity/virginia-beach/hrsd-utility-payment-due-dates-extended-for-november-december-bills/291-f374d34d-d89e-4556-b056-36fafc5c7b7e
14. News Release - January 6, 2021 | HRSD, accessed April 29, 2025, http://www.hrsd.com/news-release-january-6-2021
15. HRSD, HRUBS Bill Payment Due Dates for November & December Bills Extended to Jan 31 without Penalty - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicAlerts.asp?AID=5269&ARC=10298
16. FAQs HRSD Ransomware Attack - Norfolk.gov, accessed April 29, 2025, https://www.norfolk.gov/DocumentCenter/View/63811/FAQs-HRSD-Ransomware-Attack

17. COMMISSION MEETING MINUTES December 15, 2020 - HRSD, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/Commission_Minutes/2020/12-15-2020FINALCommissionMinutes.pdf
18. HRUBS Billing Statements Delayed - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicSend/ViewMessage/message/131470
19. Critical Infrastructure — The Ransomware Files - Apple Podcasts, accessed April 29, 2025, https://podcasts.apple.com/us/podcast/critical-infrastructure/id1593282775?i=1000544373431&l=ru
20. COMMISSION MEETING MINUTES November 22, 2022 - HRSD, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/Commission_Minutes/2022/11-22-2022FINALCommissionMinutes(3).pdf
21. COMMISSION MEETING MINUTES November 22, 2022 - HRSD, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/Commission_Minutes/2022/11-22-2022FINALCommissionMinutes.pdf
22. Revised 05/22/2024* HRSD Commission Meeting Agenda 9:00 a.m. – May 28, 2024 In-person for Commissioners and essential staff at, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/commission_agendas/2024/05-28-2024CommissionAgenda-rev05222024.pdf
23. Compromise of U.S. Water Treatment Facility - CISA, accessed April 29, 2025, https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a
24. How Cyber-Attacks Take Down Critical Infrastructure - Darktrace, accessed April 29, 2025, https://darktrace.com/blog/how-cyber-attacks-take-down-critical-infrastructure
25. Management, Operations, and Maintenance (MOM) Program - HRSD, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/EPA/HRSD_MOM_Program_Updated-July2021.pdf
26. Events | Virginia Section American Water Works Association, accessed April 29, 2025, https://vaawwa.org/events?searchtypes=none&from=2024%2F07%2F10&to=2021%2F12%2F31
27. HRSD, accessed April 29, 2025, https://www.hrsd.com/node?page=82
28. The Ransomware Files, Episode 3: Critical Infrastructure, accessed April 29, 2025, https://www.nacwa.org/news-publications/news-detail/2021/12/10/the-ransomware-files-episode-3-critical-infrastructure
29. James River Treatment Plant-SWIFT Facility Virtual Presentation (December 2020) - HRSD, accessed April 29, 2025, https://www.hrsd.com/node?page=85
30. HRSD, HRUBS Bill Payment Due Dates for November & December Bills Extended to Jan 31 Without Penalty - JCC Alert, accessed April 29, 2025, https://www.jccalert.org/CivicAlerts.aspx?AID=4407

31. COMMISSION MEETING MINUTES November 23, 2021 - HRSD, accessed April 29, 2025, https://www.hrsd.com/sites/default/files/assets/Documents/pdfs/Commission_Minutes/2021/11-23-2021FinalCommissionMinutesRev.pdf
32. Payment Methods - HRSD, accessed April 29, 2025, https://www.hrsd.com/payment-methods
33. HRSD, HRUBS Bill Payment Due Dates for November & December Bills Extended to Jan 31 Without Penalty - James City County, accessed April 29, 2025, https://www.jamescitycountyva.gov/CivicAlerts.aspx?AID=4407
34. Update Billing Agent and Apply for Hardship Advances Change Healthcare Cyberattack, accessed April 29, 2025, https://medicaid.ncdhhs.gov/blog/2024/03/08/update-billing-agent-and-apply-hardship-advances-change-healthcare-cyberattack
35. Frederick Health Hospital Faces 5 Lawsuits Following Ransomware Attack, accessed April 29, 2025, http://www.healthcarefacilitiestoday.com/posts/Frederick-Health-Hospital-Faces-5-Lawsuits-Following-Ransomware-Attack--30248
36. Human Behavior AI Protects Hampton Roads Sanitation District Ecosystems - Abnormal Security, accessed April 29, 2025, https://files.abnormalsecurity.com/production/files/HRSD-Customer-Case-Study.pdf?dm=1727116930
37. Page 87 - Latest News in Security Operations > Incident & Breach, accessed April 29, 2025, https://www.databreachtoday.com/latest-news/incident-breach-response-c-40/p-87
38. Smithfield, Surry utility bills impacted by ransomware, accessed April 29, 2025, https://www.smithfieldtimes.com/2020/12/15/smithfield-surry-utility-bills-impacted-by-ransomware/
39. US House Committee calls for offensive cyber strategies in response to rising adversarial threats, accessed April 29, 2025, https://industrialcyber.co/critical-infrastructure/us-house-committee-calls-for-offensive-cyber-strategies-in-response-to-rising-adversarial-threats/
40. Information Security | Ministry of Human Resources and Social Development, accessed April 29, 2025, https://www.hrsd.gov.sa/en/729863
41. "First 48": What to Expect When a Cyber Incident Occurs, November 2022 - CISA, accessed April 29, 2025, https://www.cisa.gov/sites/default/files/2024-09/24_0828_safecom_first_48_what_expect_when_cyber_incident_occurs_2022_final_508C.pdf
42. Round Table Discussion: Cyber Incidents and the Public Sector (HRSD Ransomware Incident) VA AWWA/VWEA ITC Meeting 05/20/2021, accessed April 29, 2025, https://www.des.sc.gov/sites/scdph/files/media/document/BOW_Cybersecurity_HRSDRoundTableDiscussion.pdf
43. Page 113 - Latest News in Fraud Management & Cybercrime, accessed April 29,

2025, https://www.govinfosecurity.com/latest-news/cybercrime-c-416/p-113
44. HRUBS Statements Delayed due to November 2020 HRSD Ransomware Attack - City of Norfolk, accessed April 29, 2025, https://www.norfolk.gov/CivicAlerts.asp?AID=5215&ARC=10212
45. Cyber Case Study: UVM Health Network Ransomware Attack - insurica, accessed April 29, 2025, https://insurica.com/blog/uvm-health-network-ransomware-attack/
46. Fact Sheet: Ransomware and HIPAA - HHS.gov, accessed April 29, 2025, https://www.hhs.gov/hipaa/for-professionals/security/guidance/cybersecurity/ransomware-fact-sheet/index.html
47. Ransomware and Recovery Time: What You Should Expect - Cigent, accessed April 29, 2025, https://www.cigent.com/blog/ransomware-and-recovery-time-what-you-should-expect
48. A Recovery Guide to Ransomware: Crucial Questions Answered - Pentest People, accessed April 29, 2025, https://www.pentestpeople.com/blog-posts/a-recovery-guide-to-ransomware-crucial-questions-answered
49. Ransomware Attack Recovery Plan and Strategy : r/sysadmin - Reddit, accessed April 29, 2025, https://www.reddit.com/r/sysadmin/comments/17rinqq/ransomware_attack_recovery_plan_and_strategy/