Data Breach on a Los Angeles Unified School District (LAUSD)

Suraj Khadka
skhadka9@gatech.edu

***Abstract*—** In September 2022, The Russian hacking group known as Vice Society carried out a data breach at the Los Angeles Unified School District, LAUSD, California. The breach compromised the data of over 400,000 students and 1000 schools, exposing sensitive information to the public domain by exploiting vulnerabilities in LAUSD's remote access system. Using the Diamond Model framework, it explains the roles of the attacker, victim, infrastructure, capability, and socio-political and technological characteristics in the breach. Policy assessments focus on the importance of creating specific plans to protect schools from cyber attacks. These plans include things like training on how to stay safe online, keeping computer programs up to date, using more than one way to log in securely, preparing for how to handle a cyber attack, and working together with police and cyber security groups. These steps will help make schools more secure against changing cyber dangers.

1 INCIDENT DESCRIPTION

In September 2022, the Los Angeles Unified School District (LAUSD) faced a massive data breach caused by the Russian criminal hacking group called Vice Society. This breach, considered one of the biggest in the education field, had far-reaching consequences on the district's activities affecting about 1000 schools, and approximately 400,000 students. The cyber attack gained access by exploiting a vulnerability in the district's remote access system. LAUSD's computer systems were compromised, blocking access to data and programs during the Labor Day weekend.

The breach exposed a volume of data estimated at around 500 GB encompassing a diverse range of vital information essential to the LAUSD operations. The compromised data included a range of details such as names, addresses, phone numbers, email addresses, passport information, and employee social security numbers. Moreover, the breach revealed records, banking information, and health data including COVID-19 vaccination records, background checks and conviction reports, VPN login details, contracts, legal papers, and employee account credentials.

Following the data breach, LAUSD actively looked for guidance from the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA). Despite Vice Society asking for ransom, LAUSD chose not to give in to the demand. As a result, the Vice Society made more than 200,000 files public on the dark web.

The incident caused daily disruptions to district operations and sparked worries about the security of private data that educational institutions hold. The LAUSD was allegedly careless in fixing known vulnerabilities in its systems before the attack, which could have resulted in legal consequences. After the compromise, the district was forced to consider the ramifications of hacked data as well as the possible long-term effects on stakeholders, employees, and students.

2 DIAMOND MODEL

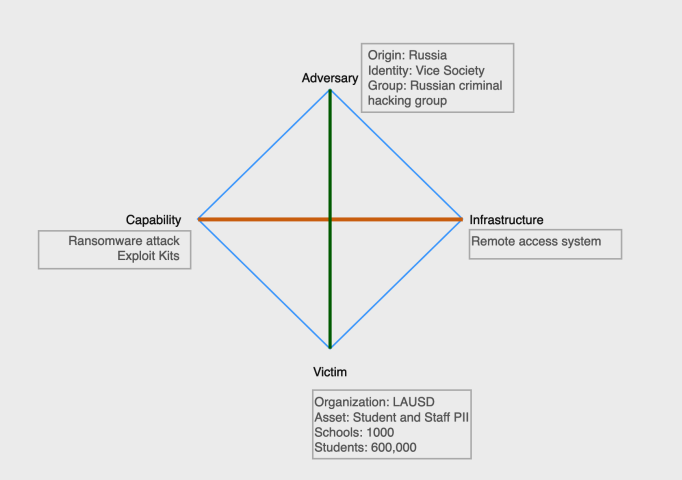

Figure 1—LAUSD Diamond Model

2.1 Adversary

The attack on the Los Angeles Unified School District (LAUSD) was carried out by a notorious Russian criminal hacking group, called Vice Society. This group is motivated by financial gain and typically employs ransomware extortion attacks as a means of extracting substantial sums of money from their victims.

The vice society employs different tactics in accomplishing their operations. Among the strategies used are taking advantage of loopholes in system architecture, using social engineering to gain legal access, and using ransomware to encrypt sensitive data and force people to pay the money demanded. They aim to inflict as much disruption as they can and compel their victims to do what they want by executing their attacks precisely with the specific timing. Vice Society also enjoys the anonymity that the dark web offers them to communicate with their targets as well as to make the ransom payment conveniently, which allows the law authorities to trace and capture them.

2 .2Victim

The primary victim was the Los Angeles Unified School District (LAUSD). LAUSD operates more than 1000 schools and serves around 400,000 students, making it a prime target for cybercriminals seeking to exploit vulnerabilities within its extensive network.

The LAUSD was vulnerable to cyber attacks because of its inadequate cyber security posture and its absence of active risk management processes. The district's systems were vulnerable to attacks because warnings about possible weaknesses in the system were ignored, and necessary security updates were not applied. Moreover, the vast operations within the LAUSD network probably made it difficult to manage strict control and strong security mechanisms against skilled cyber adversaries. The district worked with federal agencies like CISA and the FBI to block the infiltration but was unable to stop the attack, highlighting the district's inadequate cyber security posture.

2.3 Infrastructure

Several systems, networks, and assets in the Los Angeles Unified School District were targets of the ransomware attack. These included:

2.3.1 Personal Information Database

One of the main objectives of the attack was the database of LAUSD. This database contained the names, physical addresses, phone numbers, passport information, and social security numbers of both employees and students. The data breach of this database posed serious privacy and security threats for individuals affected by the attack.

2.3.2 *Email Systems and Applications*

The district's capacity to coordinate response activities and deliver vital services to students, parents, and staff members was hampered by the ransomware assault, which also affected LAUSD's email systems and applications.

2.3.3 *Computer Systems and Networks*

Vice society infiltrated several computer systems and networks within the LAUSD's infrastructure, making them unusable and interfering with regular operations throughout the district's educational establishments.

2.3.4 *Financial and Administrative Records*

The ransomware attack targeted several assets, including financial reports, banking information, tax forms, contracts, legal documents, and employee account login information of LAUSD. The school system may suffer serious legal, financial, and reputational repercussions from the theft and possible release of this private information.

2.3.5 *Student Data*

Psychiatric evaluations, health records (including COVID-19 immunization records), and VPN login credentials were among the student data stolen by the hack. The disclosure of such information raises concerns about privacy violations,

identity theft, and other forms of exploitation aimed at students, employees, and their families.

2.4 Capability

Vice Society, the attackers, showed their ability to plan a complex cyber attack when they carried out the ransomware attack against the Los Angeles Unified School District (LAUSD). To successfully execute the attack, the adversary used a variety of instruments, strategies, and assets. First, Vice Society made use of internal login credentials that had been leaked, including those for the Virtual Private Network (VPN) of the Los Angeles Unified School District (a vital point of entry into the district's network infrastructure). After gaining access to the VPN, the attackers were able to spread their ransomware to other vulnerable areas of the network while also gaining a foothold within it.

In addition, the attackers were able to exploit the district's cyber security defenses by finding and taking advantage of weaknesses in the remote access system of LAUSD. This indicates a degree of technological know-how and reconnaissance on the side of the attackers, enabling them to identify vulnerabilities and accomplish their goals.

2.5 Social-Political Meta-Feature

Numerous social and political elements affect the interaction between the victim (LAUSD) and the adversary (Vice Society). From a societal point of view, attacking a major school system such as the Los Angeles Unified School District not only disrupts vital services but also undermines faith in educational institutions. Upon learning that their personal information has been hacked, parents, teachers, and students may feel vulnerable and uneasy. The incident emphasizes the necessity of improved cyber security measures in educational institutions and raises concerns about the broader effects of cyber attacks on public services and essential infrastructure.

From a political point of view, the incident highlights how challenging it is for organizations like LAUSD to protect sensitive information and combat cyber attacks. It also emphasizes the importance of national cyber security laws and

policies to address vulnerabilities and reduce the risk of further attacks. For example, the LAUSD may lack the necessary processes and policies to manage cyber security risks within the organization if it continues to ignore known vulnerabilities despite warnings. Furthermore, the presence of the Russian criminal hacking gang poses geopolitical questions about international cooperation and the implementation of cybercrime laws. To enhance cyber security resilience and protect critical infrastructure from cyber attacks, comprehensive policies that consider these social and political factors must be developed.

2.6 Technology Meta-Feature

It is crucial to understand the various facets of technology that support the capabilities and infrastructure involved in the data breach of the Los Angeles Unified School District (LAUSD) to comprehend the workings of the attack. By taking advantage of vulnerabilities in the LAUSD remote access system, the attackers were able to gain illegal access to the district's network. An essential first step in carrying out their ransomware attack was for the attackers to get a foothold in the network by breaking into the district's Virtual Private Network (VPN). Organizations frequently employ VPNs to enable safe remote access to internal resources. However, VPNs can turn into weak points of access for hackers if they are not well-guarded and observed.

Second, the district's network was encrypted by the ransomware attack, which used advanced encryption methods. This highlights the necessity for strong endpoint security solutions that can identify and mitigate ransomware assaults in real time. It also shows that the adversaries are using sophisticated malware and encryption algorithms.

3 POLICY ASSESSMENT AND RECOMMENDATIONS

3.1 Level of Organization: Organizational (8)

The LAUSD data breach underscores the need for immediate policy action at the organizational level. Although the incident has broader implications for national and international cyber security, addressing vulnerabilities in educational

institutions requires local strategies tailored to the unique challenges faced by these organizations.

3.2 Assessment

3.2.1 Frequency and Severity

Ransomware attacks that target educational institutions are becoming more frequent and severe, posing serious dangers to employee and student data, operational continuity, and public trust. The LAUSD hack, which impacted hundreds of thousands of students and staff and exposed a vast array of private data, shows the magnitude of these attacks.

Table 3.2.1—Top 5 educational data breaches in the US from 2005 to 2023.

State	# of Breaches	# of Records Affected	# of Records Impacted per Student
New York	691	1M	0.25
California	303	3M	0.31
Texas	116	2.3M	0.30
Massachusetts	100	1.8M	1.25
Illinois	86	725.3K	0.25

3.2.2 Risks and Available Tools

Academic institutions are generally weak targets because they lack the resources and cyber security safeguards necessary to fend off sophisticated cyber attacks. These risks can be reduced by using policy instruments like increased financing for cyber security initiatives, required security evaluations and protocols for educational systems, and cooperation between government agencies and stakeholders in education.

3.3 Recommendations

3.3.1 Cybersecurity Training and Awareness

To ensure that staff and students can identify and properly address such risks, LAUSD must prioritize cyber security training and awareness initiatives. Educating users about phishing schemes, password security, and data protection best practices is one way to reduce the likelihood of future breaches.

3.3.2 Patch Management and Vulnerability Remediation

To lessen the possibility of adversaries exploiting known vulnerabilities in systems and applications, strong patch management procedures should be put in place and vulnerabilities should be addressed as soon as they are discovered. To enhance the security risks of LAUSD's systems and improve their resilience against cyber attacks, it is important to regularly upgrade its systems and software.

3.3.3 Multi-Factor Authentication (MFA)

Enforcing Multi-Factor Authentication (MFA) across the entire network architecture of LAUSD can provide an extra layer of security, making it more challenging for adversaries to gain unwanted access—even with compromised credentials. Multi-factor authentication (MFA) enhances authentication systems and reduces the risk of stolen credentials.

3.3.4 Incident Response Plan

For LAUSD to effectively mitigate and recover from cyberattacks, an incident response plan must be developed and tested regularly. The impact of breaches can be reduced and a coordinated response to cyber incidents can be ensured by establishing defined procedures for incident identification, containment, and recovery from security breaches.

3.3.5 Collaboration with Law Enforcement and Cybersecurity Agencies

To exchange threat information, the best practices, and resources for thwarting cyber attacks, LAUSD should partner with cyber security professionals, law enforcement agencies, and business partners. LAUSD's resilience and response

skills can be improved by forming collaborations within the cyber security community.

4 REFERENCES

1. Ansari, T. (2022, September 6). *Los Angeles schools hit with Ransomware attack - WSJ*. The Wall Street Journal. https://www.wsj.com/articles/los-angeles-schools-hit-with-ransomware-attack-11662498999
2. Cook, S. (2023, April 3). US schools leaked 32 million records in 2,691 data breaches. *comparitech*. 2024, https://www.comparitech.com/blog/vpn-privacy/us-schools-data-breaches/
3. GovTech. (2022, September 9). *Private data of 400K LAUSD students could be at risk*. GovTech. https://www.govtech.com/education/k-12/private-data-of-400k-lausd-students-could-be-at-risk
4. Greig, J. (2023, January 23). *Los Angeles Unified School District confirms SSNS leaked in September ransomware attack*. The Record from Recorded Future News. https://therecord.media/los-angeles-unified-school-district-confirms-ssns-leaked-in-september-ransomware-attack
5. Harter, C. (2023, February 23). *LAUSD cyberattack far worse than reported, 2,000 students compromised*. Daily News. https://www.dailynews.com/2023/02/22/lausd-cyberattack-far-worse-than-reported-with-2000-students-compromised/
6. Hope, A. (2022, September 15). *FBI and CISA responded to a cyber attack and ransomware incident on Los Angeles School District (LAUSD)*. CPO Magazine. https://www.cpomagazine.com/cyber-security/fbi-and-cisa-responded-to-a-cyber-attack-and-ransomware-incident-on-los-angeles-school-district-lausd/
7. Kapko, M. (2023). Los angeles school district confirms sensitive student data leaked. *Cybersecurity Dive,* Retrieved from https://www.proquest.com/trade-journals/los-angeles-school-district-confirms-sensitive/docview/2783530667/se-2
8. Kaplan, C. (2022, December 7). *The second largest school district in the U.S. falls victim to cyberattack*. HALOCK. https://www.halock.com/the-second-largest-school-district-in-the-u-s-falls-victim-to-cyberattack/
9. Kost, E. (2023, March 2). *How did lausd get hacked in 2022?: Upguard*. RSS. https://www.upguard.com/blog/how-did-lausd-get-hacked
10. Los Angeles Unified Targeted by Ransomware Attack. (2022, September 5). *LAUSD UNIFIED*. Retrieved 2024, from https://www.lausd.org/site/default.aspx?PageType=3&DomainID=4&ModuleInstanceID=4466&ViewID=6446EE88-D30C-497E-9316-3F8874B3E108&RenderLoc=0&FlexDataID=122768&PageID=1.

11. Miguel. (2022, October 3). *Los Angeles School District suffers a data breach*. IDStrong. https://www.idstrong.com/sentinel/lausd-data-breach/
12. Page, C. (2022, October 3). *Hackers leak 500GB trove of data stolen during LAUSD Ransomware attack*. TechCrunch. https://techcrunch.com/2022/10/03/los-angeles-school-district-ransomware-data/
13. Romine, T., Sanchez, R., & Razek, R. (2022, Oct 01). Cybercriminals behind los angeles unified school district ransomware attack release hacked data, superintendent says. *CNN Wire Service* Retrieved from https://www.proquest.com/wire-feeds/cybercriminals-behind-los-angeles-unified-school/docview/2719711630/se-2

5 APPENDICES

Appendix 5.1: Types of Compromised Data

Data Category	Description
Personal Information	Names, phone numbers, addresses social security numbers
Financial and administrative	Legal documents, tax forms, banking information
Email Systems and applications	User emails addresses and applications
Health Data	Psychiatric evaluations, health records, COVID-19 vaccination records
Student Data	VPN login credentials, student account login information

Appendix 5.2: Incident Response Plan

Phase	Description
Preparation	Define roles and responsibilities, develop communication channels and procedures
Identification	Detect and confirm incidents through monitoring, alert systems, or reports from users and stakeholders
Containment	Isolate impacted networks or systems to stop additional harm, lessen lingering dangers, and restrict data exposure.
Eradication	Eliminate harmful elements, repair vulnerabilities to stop recurrence, and restore impacted systems from backups.
Recovery	Restore regular operations, confirm the integrity of the system, and carry out post-event analysis to determine lessons learned.
Lessons Learned	Record results, revise incident response strategy considering lessons gained, and offer training to facilitate development.