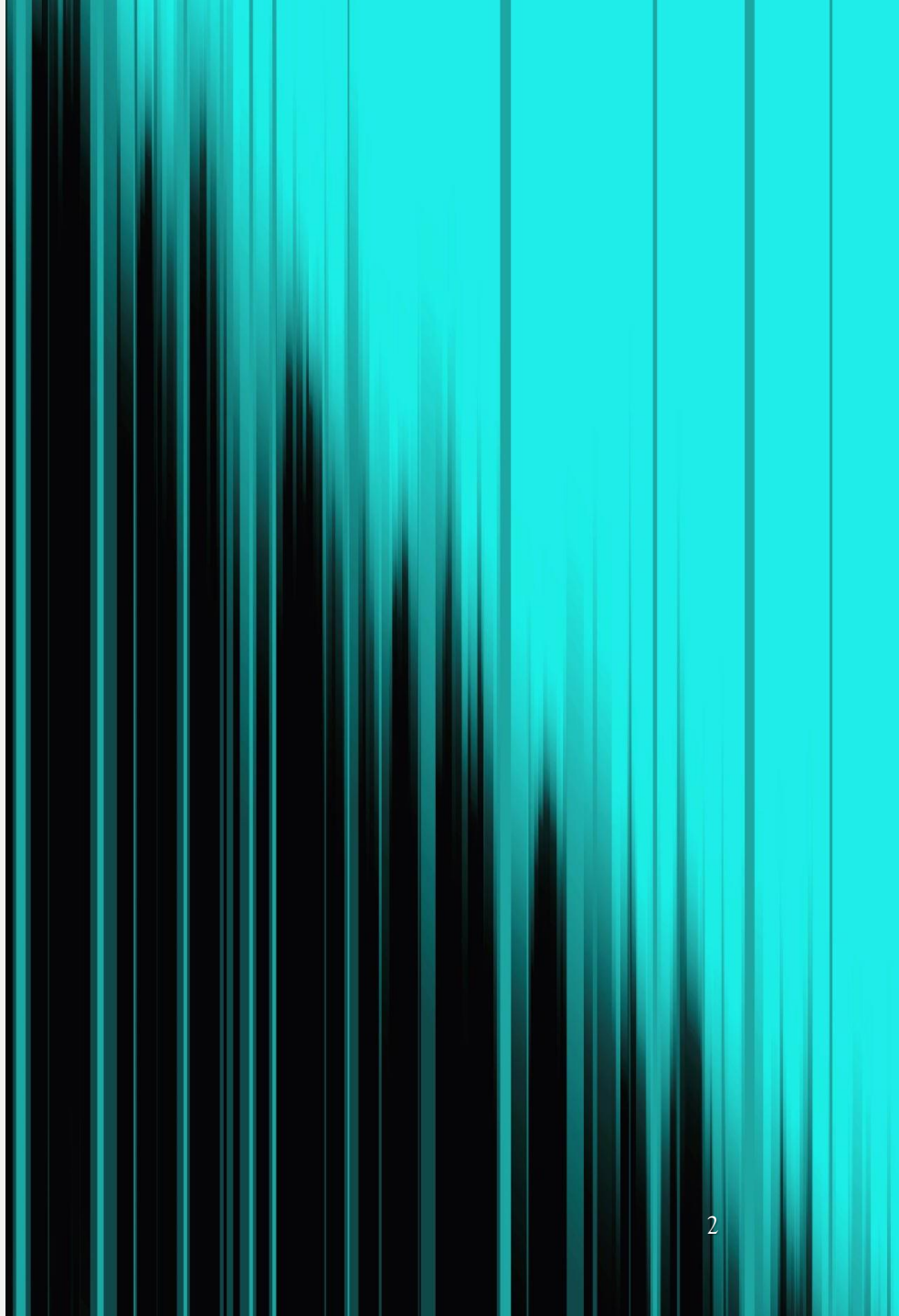
CASE STUDY OF ATTACKS ON OSI MODEL

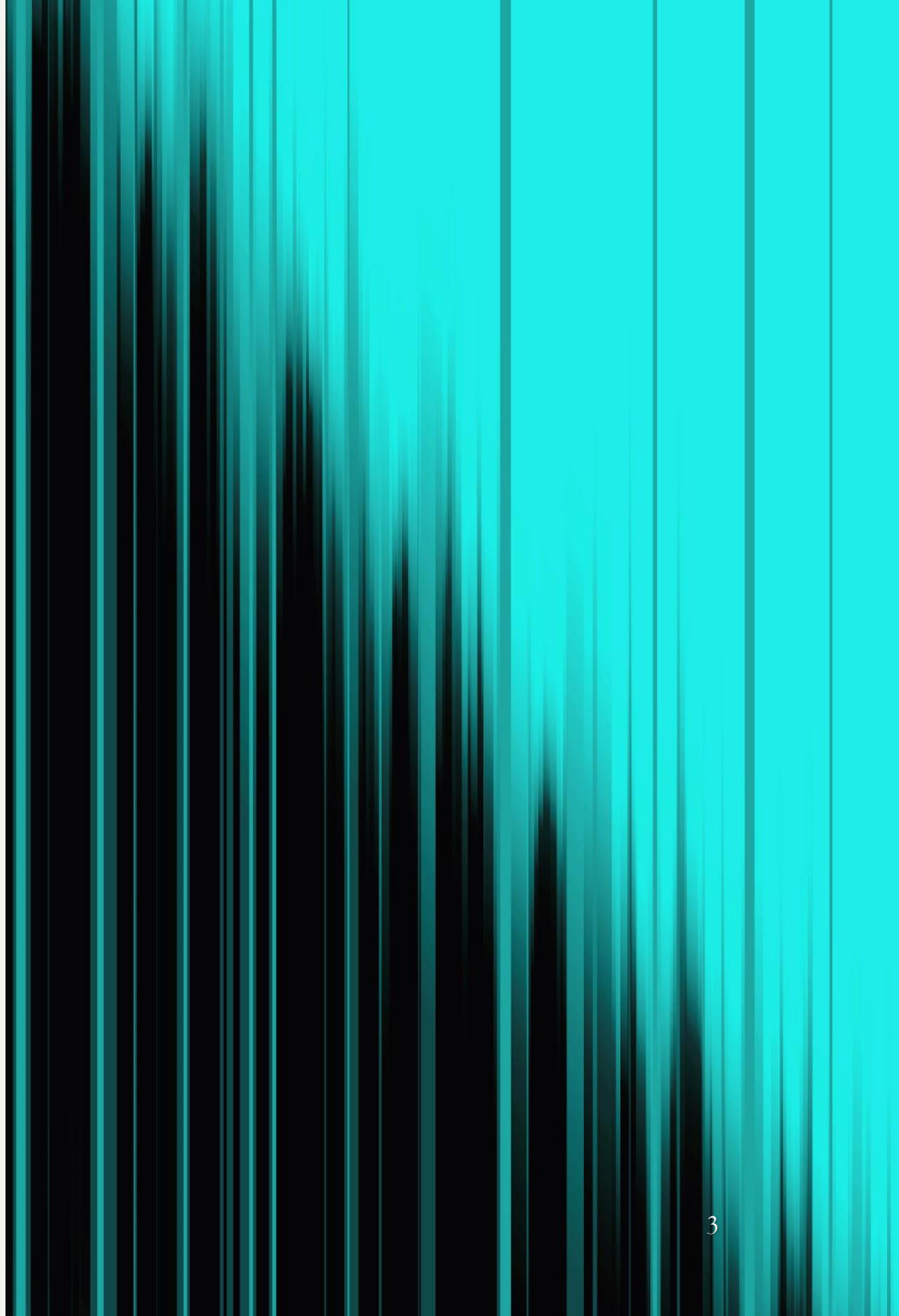
CASE STUDY1: STUXNET WORM ATTACK

The Stuxnet worm attack, discovered in 2010, targeted supervisory control and data acquisition (SCADA) systems, specifically those used in Iran's nuclear facilities. This sophisticated attack aimed to disrupt and sabotage the operation of Iran's uranium enrichment centrifuges.



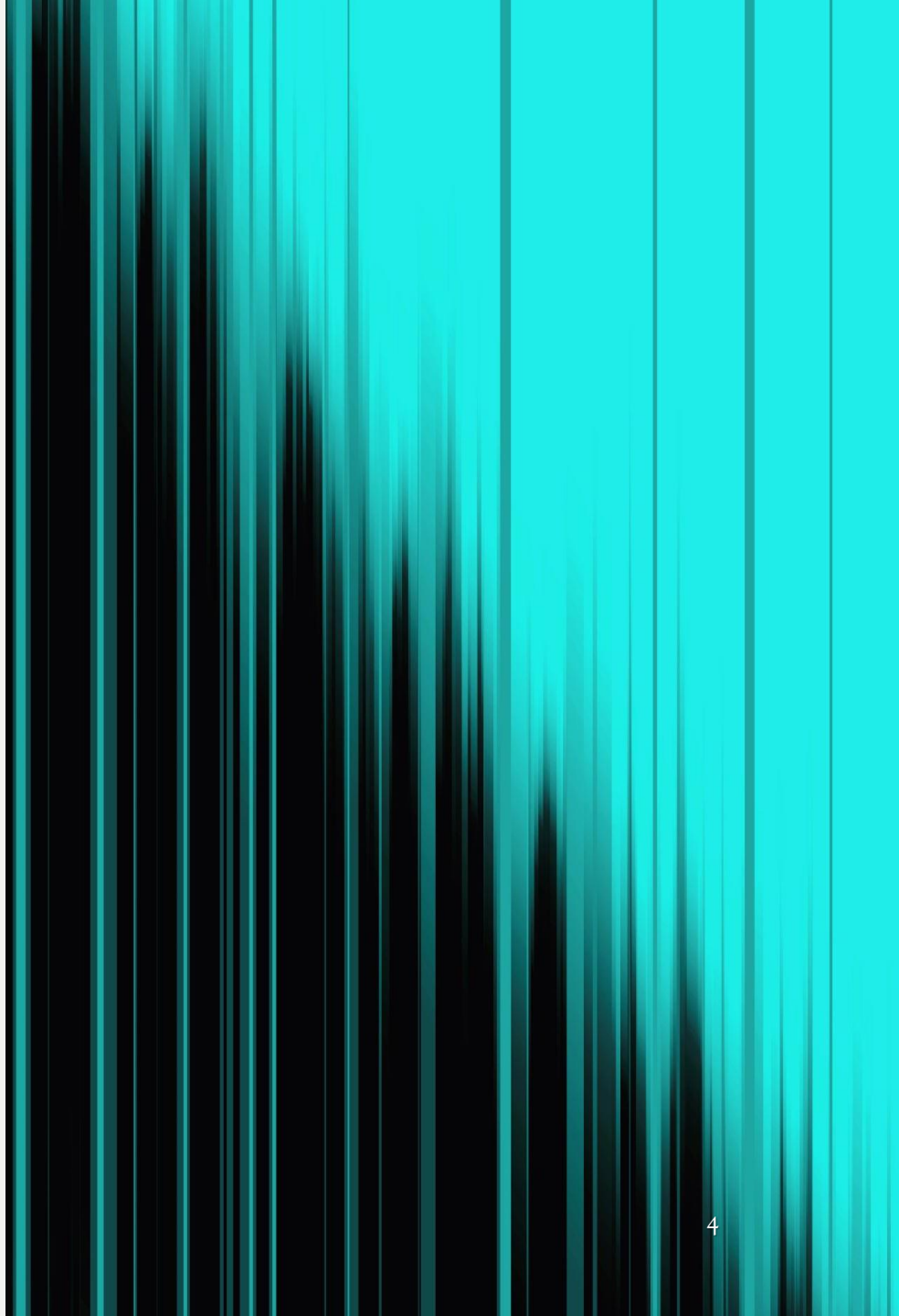
IMPACT OF STUXNET WORM ATTACK

- The Stuxnet worm attack had far-reaching consequences, demonstrating the potential for cyberattacks to disrupt critical infrastructure systems.
- It specifically targeted SCADA systems, which are responsible for monitoring and controlling industrial processes.
- The attack compromised multiple layers of the OSI model, resulting in physical damage and operational disruption.



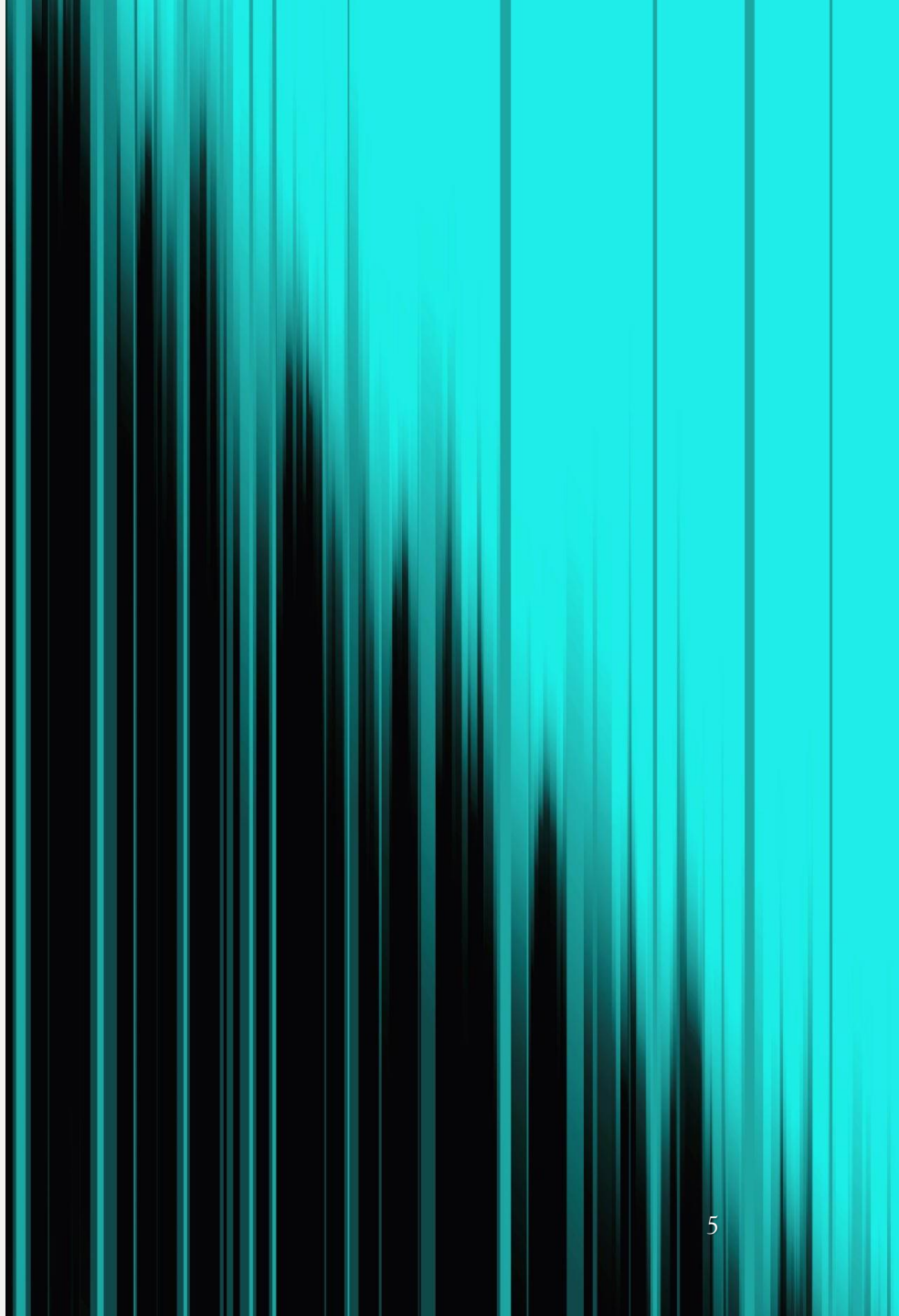
CONSEQUENCES OF STUXNET WORM ATTACK

- Physical Damage: Stuxnet targeted the physical layer (Layer 1) by exploiting zero-day vulnerabilities in Microsoft Windows to gain access to the target systems.
- Operational Disruption: Stuxnet impacted the data link layer (Layer 2) by tampering with the communication protocols used by the SCADA systems.
- Exploiting Software Vulnerabilities: Stuxnet exploited vulnerabilities in the application layer (Layer 7) by using malicious code hidden within infected files.



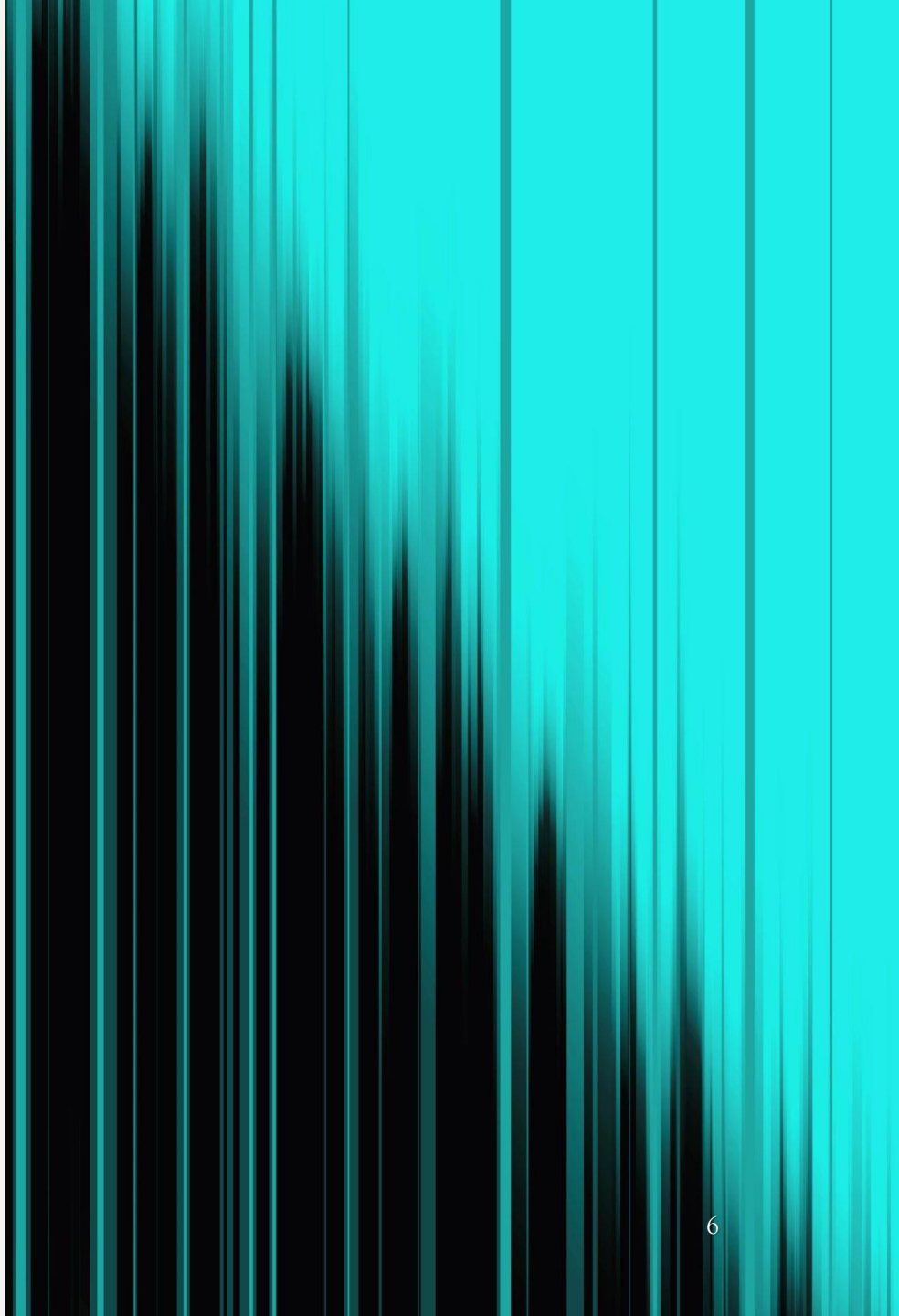
COUNTERMEASURES TO PREVENT STUXNET WORM ATTACK

- Patch Management: Regularly applying security patches and updates to all software and operating systems can mitigate the risk of vulnerabilities being exploited by attackers.
- Network Segmentation and Access Control: Implementing this helps isolate critical infrastructure systems from external networks and other less critical systems.
- Intrusion Detection and Prevention Systems: Employing these systems at various layers of the network infrastructure can help identify and block malicious activities.



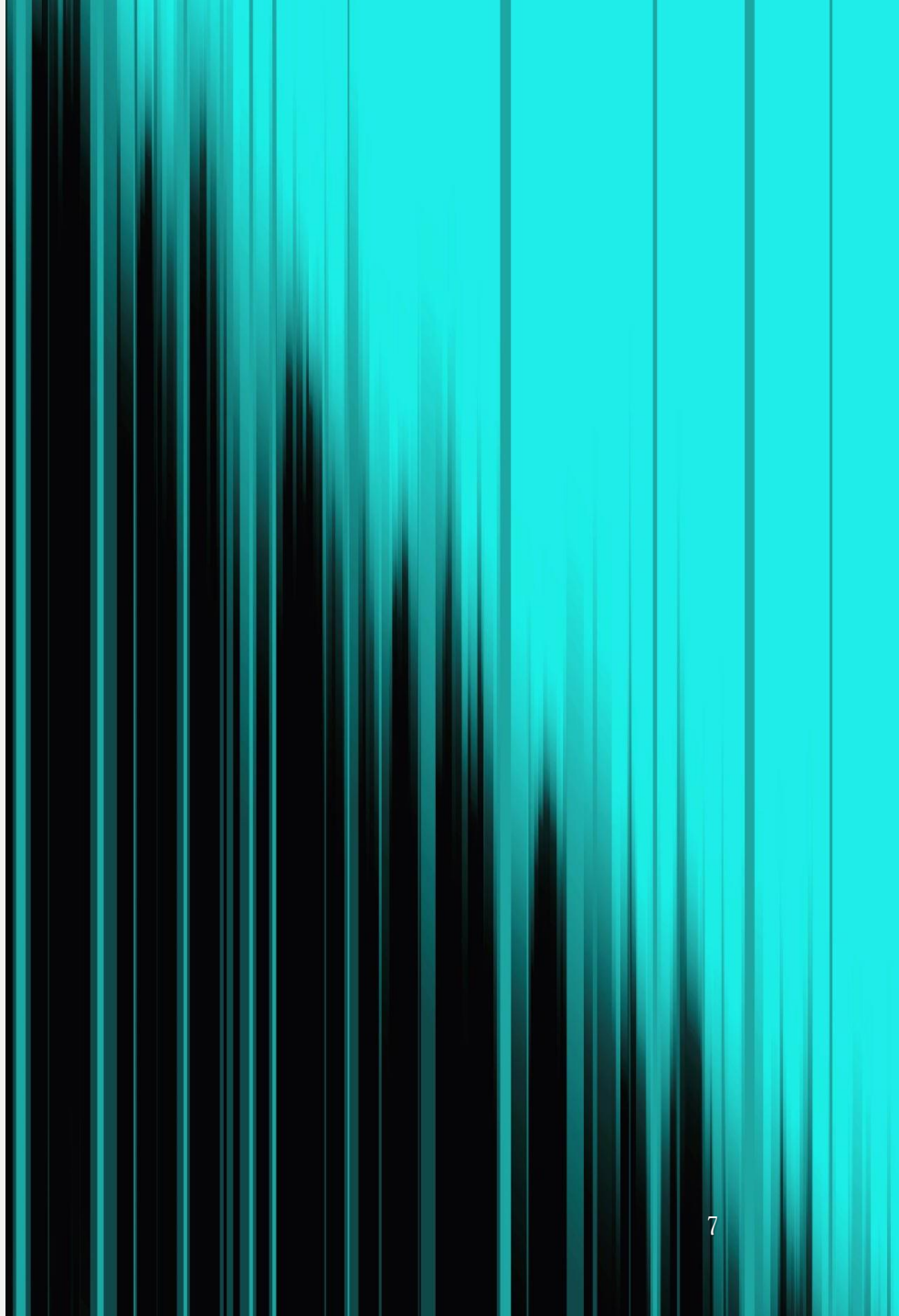
COUNTERMEASURES TO PREVENT STUXNET WORM ATTACK

- Security Awareness and Training: Training SCADA operators, system administrators, and personnel on secure practices.
- Recognizing and responding to potential cyber threats, can enhance the overall security posture.
- Education on phishing attacks, social engineering techniques, and safe computing practices helps mitigate the risk of human error leading to successful attacks.



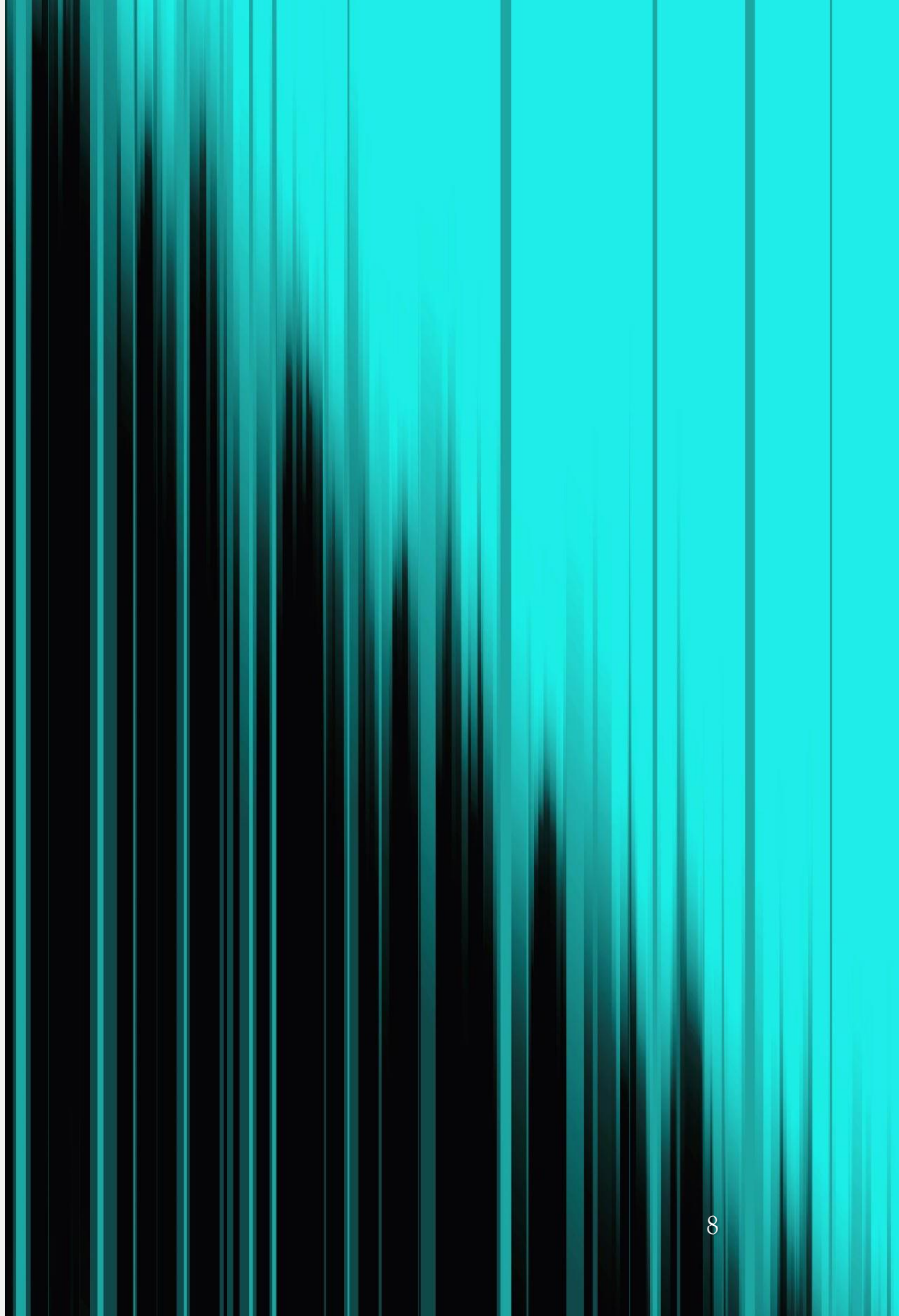
CASE STUDY2: SQL INJECTION ATTACK

SQL injection is a type of attack that targets the application layer (Layer 7) of the OSI model. It takes advantage of vulnerabilities in web applications that do not properly validate and sanitize user input before interacting with a database.



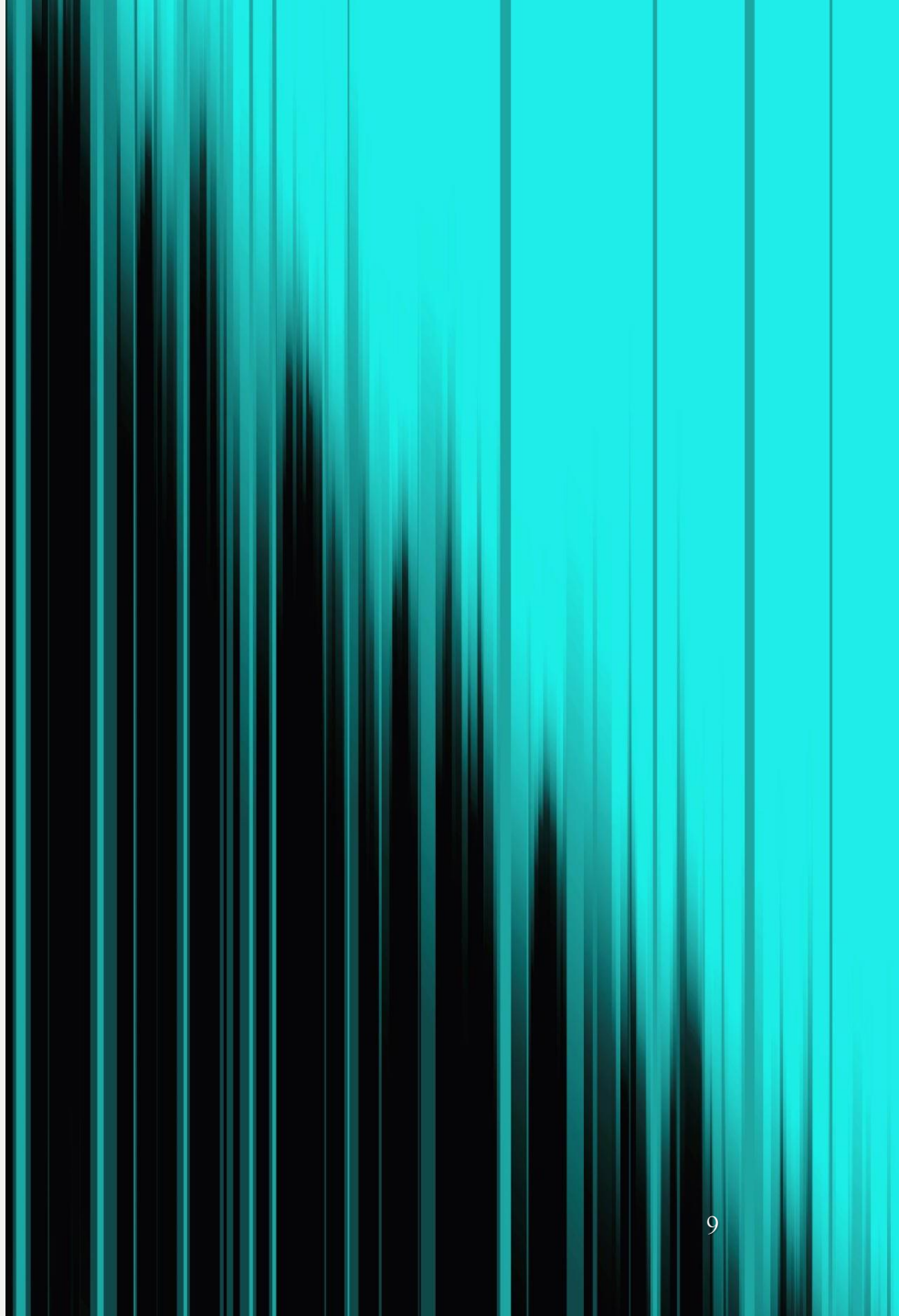
IMPACT OF SQL INJECTION ATTACK

- In 2013, the retail giant Target fell victim to a massive data breach that compromised the personal and financial information of approximately 40 million customers.
- The attack exploited a vulnerability in Target's web application, which allowed the attackers to inject malicious SQL (Structured Query Language) code into the application's input fields.
- Through this SQL injection attack, the hackers gained unauthorized access to the customer database and exfiltrated sensitive information.



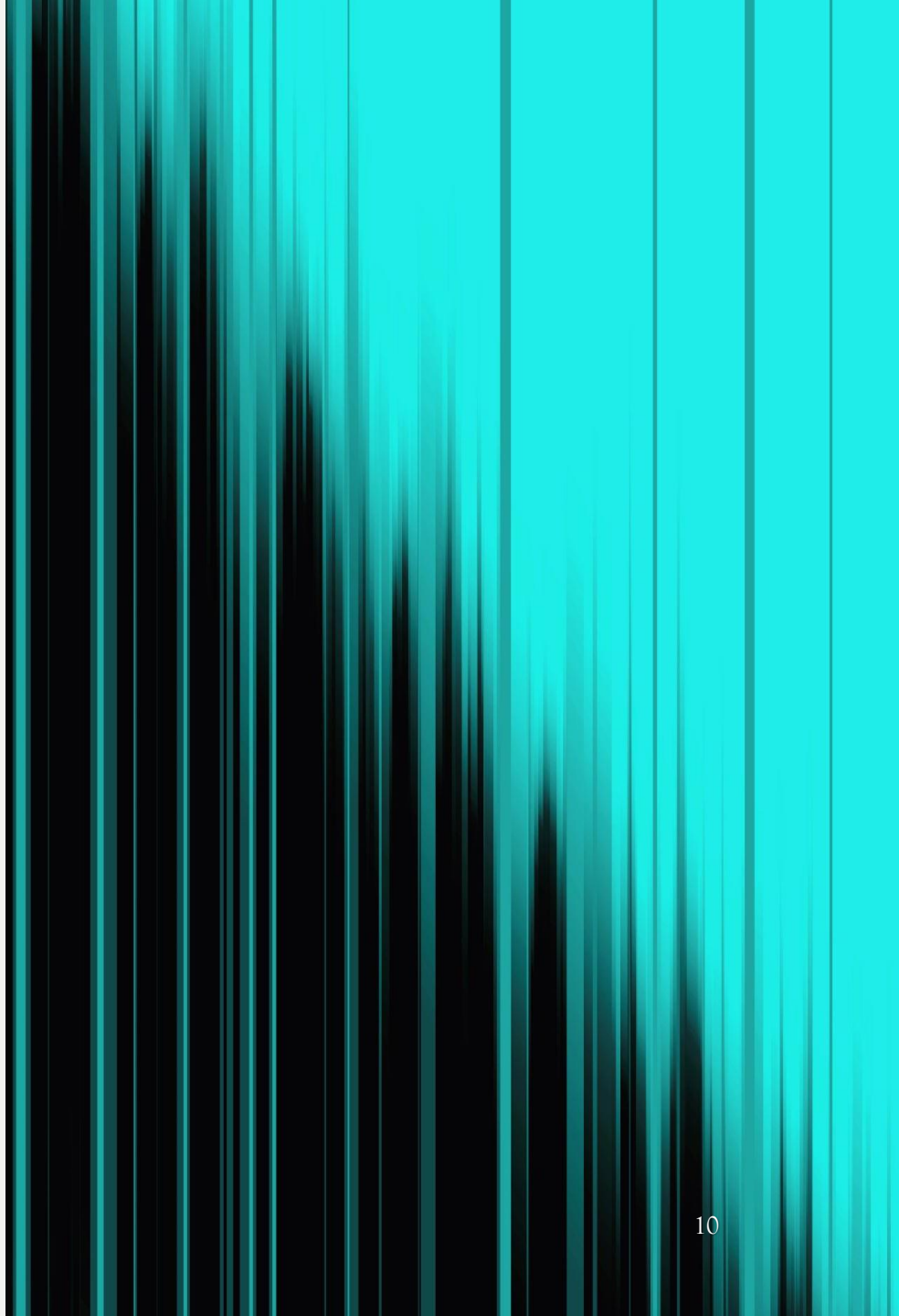
CONSEQUENCES OF SQL INJECTION ATTACK

- Data Manipulation: Malicious SQL statements can modify, delete, or insert data into the application's database, leading to data corruption or unauthorized modifications.
- Unauthorized Data Access: Attackers can bypass authentication mechanisms, retrieve sensitive information from databases, or gain unauthorized access to user accounts.
- Denial of Service: Attackers may exploit SQL injection vulnerabilities to perform resource-intensive queries, causing excessive server load and potential denial of service for legitimate users.
- Information Leakage: Error messages or debug information generated by the application during an SQL injection attack can reveal sensitive database structure, table names, or even administrator credentials, aiding future attacks.



COUNTERMEASURES TO PREVENT SQL INJECTION ATTACK

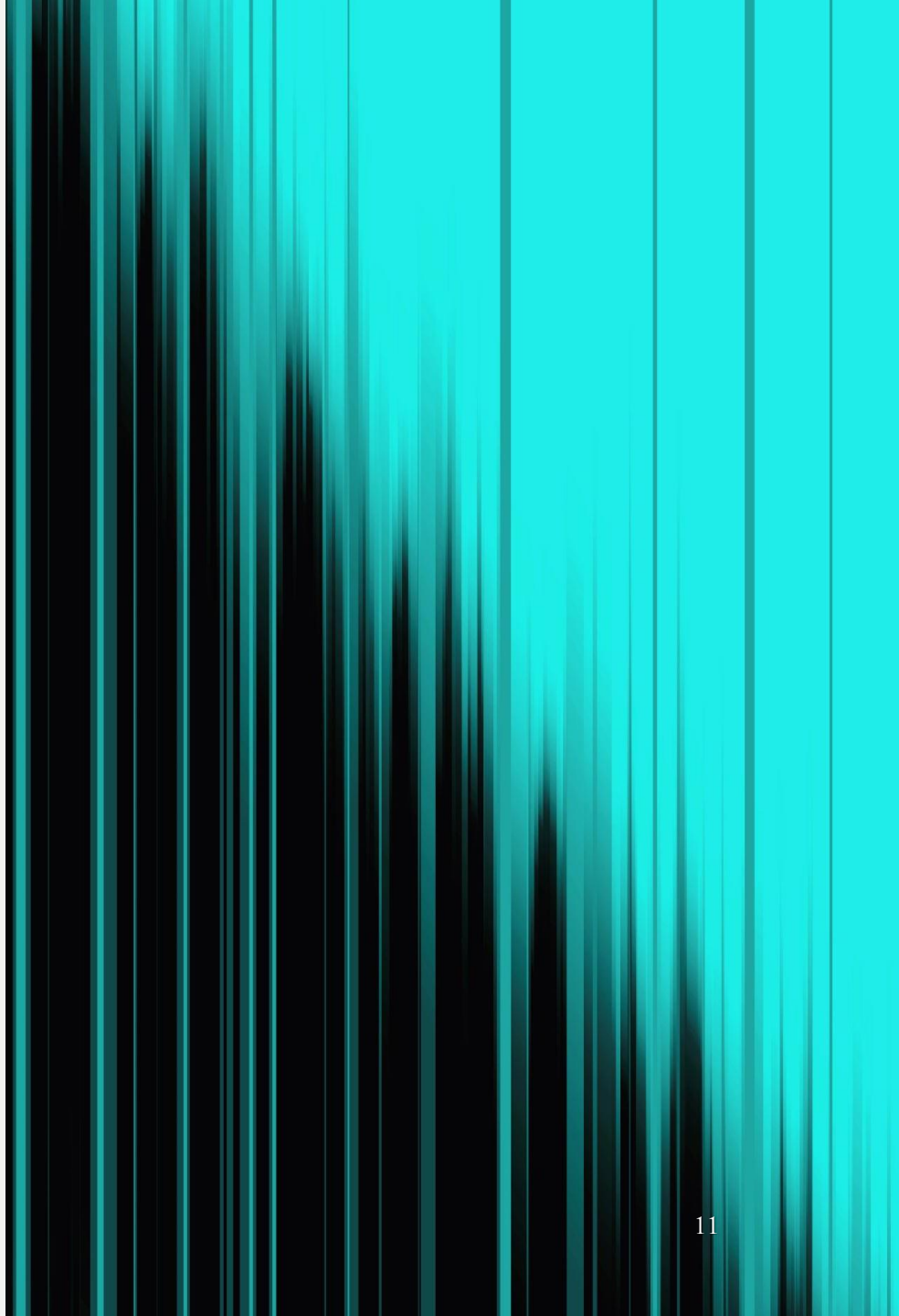
- Input Validation and Sanitization: Implement strict input validation to ensure that user input conforms to expected formats and rejects any malicious characters. Sanitize input by encoding or escaping special characters before using them in SQL queries.
- Parameterized Queries or Prepared Statements: These techniques ensure that input is treated as data rather than executable SQL, mitigating the risk of SQL injection.
- Principle of Least Privilege: Limiting access privileges reduces the potential damage an attacker can cause if an SQL injection vulnerability is exploited.



COUNTERMEASURES TO PREVENT SQL INJECTION ATTACK

- Secure Coding Practices: Implement secure coding practices, such as using built-in security libraries, and regularly updating software dependencies, to minimize the risk of introducing SQL injection vulnerabilities.

- Regular Security Testing: Perform regular security testing, including vulnerability assessments and penetration testing, to identify and address any SQL injection vulnerabilities in the application.



Type of Attack	Layer of OSI	Impact	Consequences	Counter measures	Year of attack	Impacted organization
Fiber Optic Cable Cut	Physical	Disruption of network connectivity	Loss of data transmission, service unavailability	Implementation of backup communication channels	2019	Multiple
MAC Address Spoofing	Data Link	Unauthorized network access, interception of traffic	Data compromise, network disruption	Port security measures, MAC address filtering, network access control, IEEE 802.1X	2014	Iran Nuclear
SYN Flood Attack	Transport	Server resource exhaustion, denial of service	Service unavailability, financial losses	Intrusion Prevention Systems (IPS)	2018	GitHub
SQL Injection	Application	Unauthorized data access, data modification	Compromised data integrity, unauthorized access	Input validation and sanitization	2017	Equifax
Session Hijacking	Session	Unauthorized session control, data interception	Data compromise, unauthorized access, impersonation	Secure session management	2015	Sony play station network