

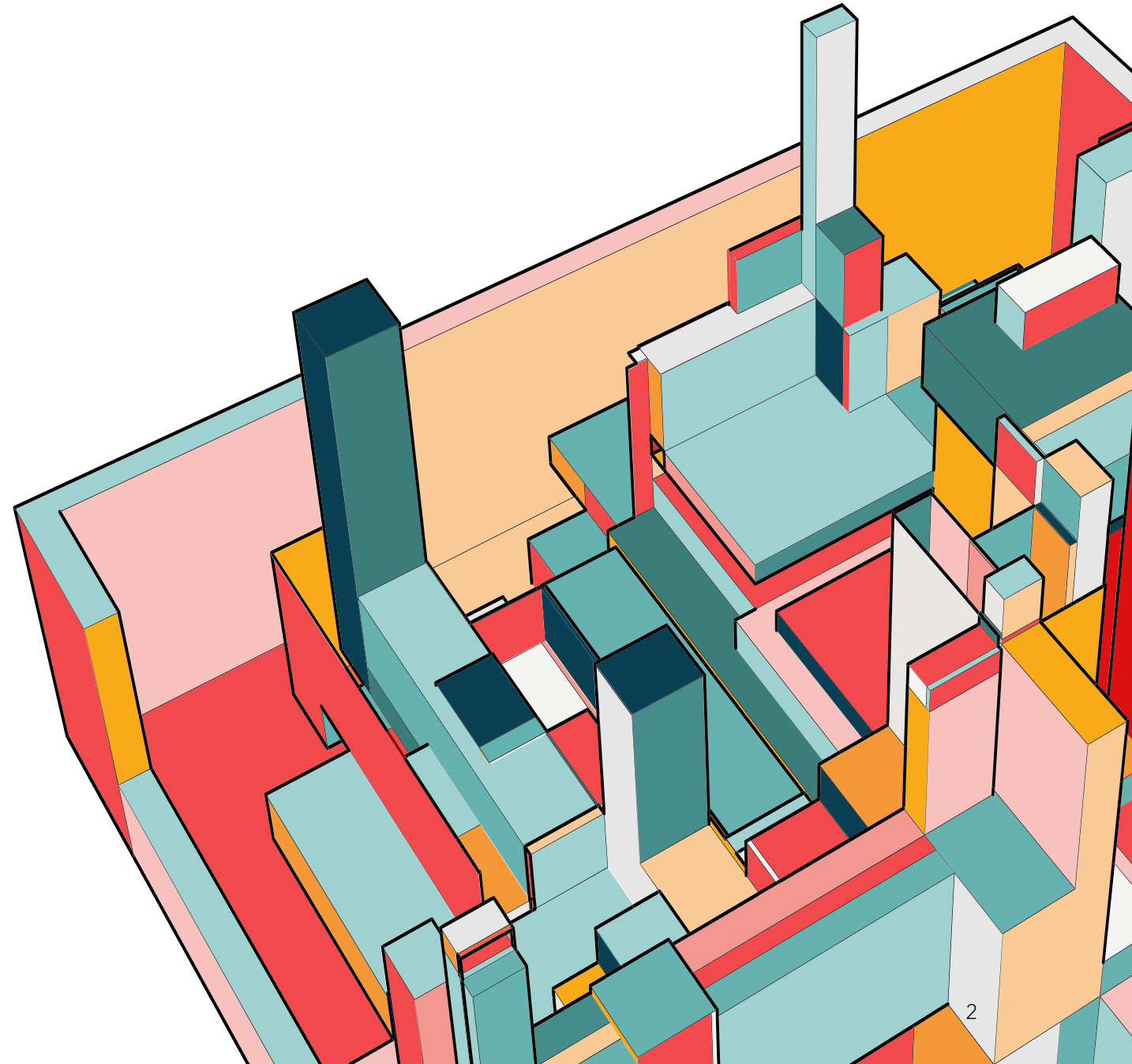


CYBER SECURITY

By Darius Moldoveanu for FinSecure Ltd
(FSL).

INTRODUCTION

FSL has faced increasing cybersecurity threats. Cybersecurity is critical to protecting customer data and business operations. This presentation summarizes key threats, security policies, mitigation measures, and recommendations to improve FSL's data security.



EXTERNAL THREATS

Phishing Attacks

Cybercriminals send fake emails posing as trusted entities to steal sensitive information (e.g., a fake IT email requesting login details).

DDoS Attacks

Attackers overwhelm our servers with traffic, shutting down online services and disrupting operations.

Supply Chain Attacks

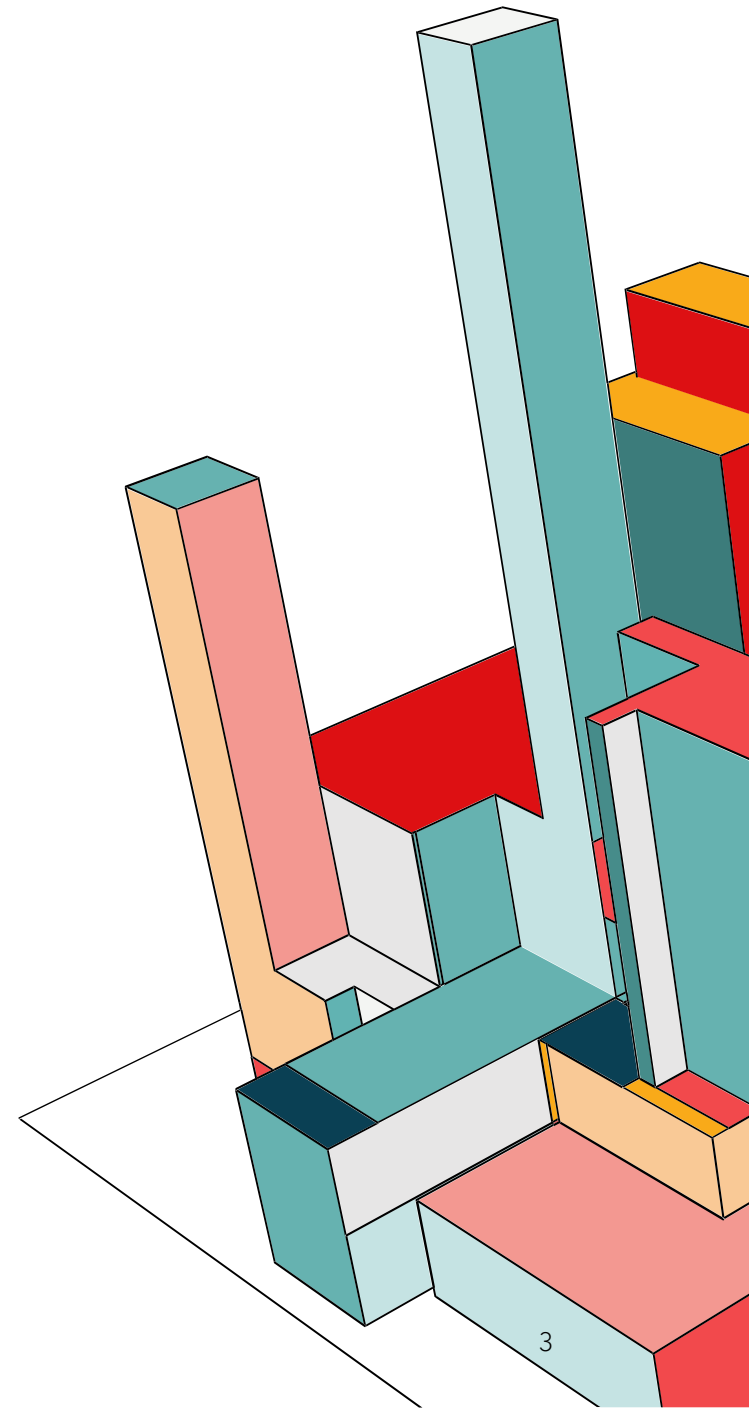
Attackers exploit vulnerabilities in third-party vendors to access our network (e.g., the SolarWinds breach).

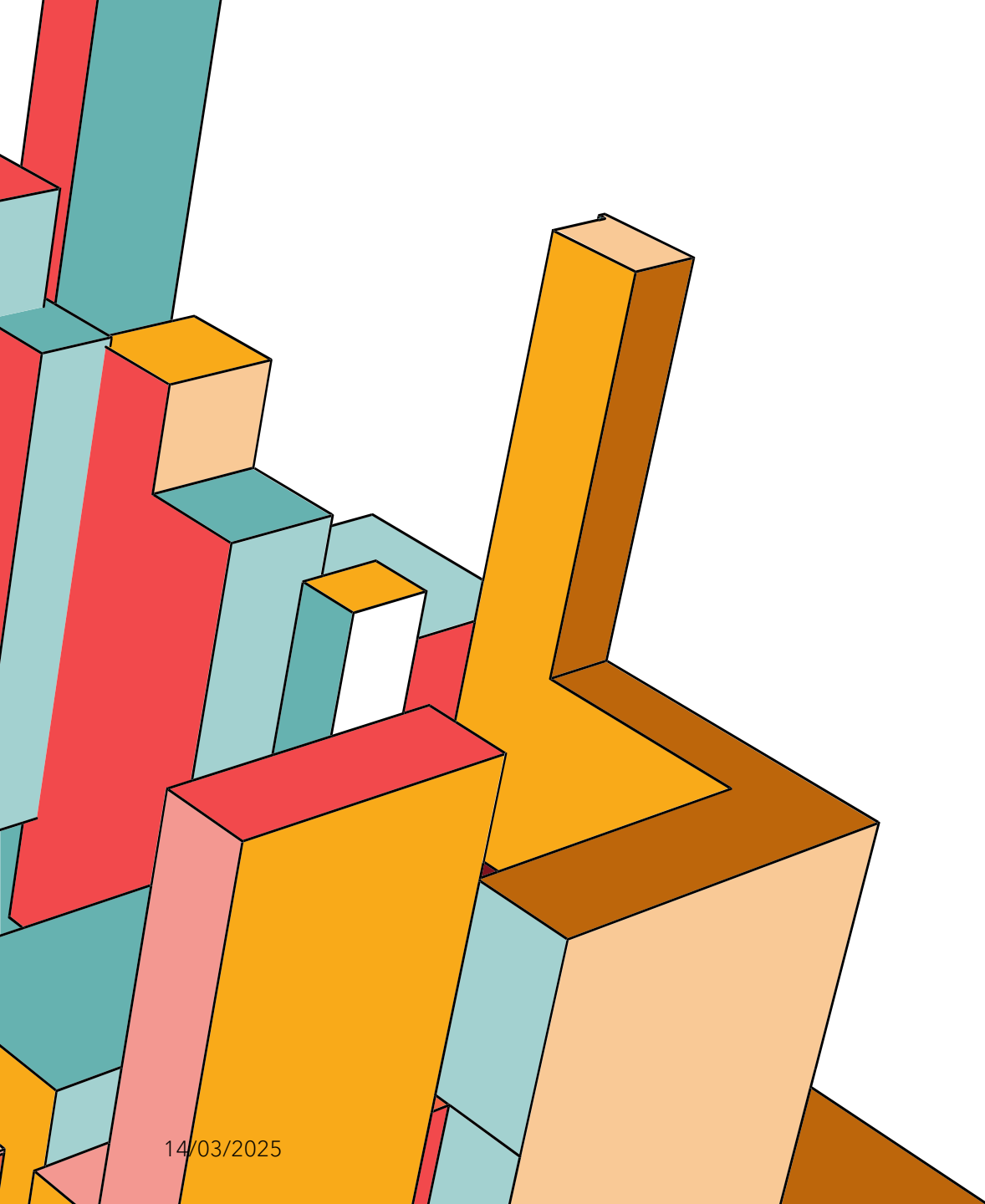
Malware & Ransomware

Malicious software that locks files or steals data, often demanding ransom payments (e.g., WannaCry ransomware attack).

Advanced Persistent Threats (APTs)

Sophisticated, prolonged attacks where hackers infiltrate systems to steal financial data over time.





INTERNAL THREATS

Insider Threats

Employees misusing access, either maliciously or by accident (e.g., an employee leaking confidential customer records).

Unauthorized Access

Weak password policies or misconfigured permissions allowing unapproved access to sensitive systems.

Data Leakage

Accidental or intentional sharing of confidential information through unsecured cloud storage, email, or removable media.

SECURITY POLICIES OVERVIEW

Information Security Policy

Defines how FSL protects its data and ensures compliance with cybersecurity best practices.

Access Control Policy

Employees only have access to the data and systems necessary for their role, minimizing exposure to risks.

Acceptable Use Policy

Provides clear guidelines on how employees can use company IT resources, ensuring responsible usage.

Incident Response Policy

Defines steps to detect, contain, and recover from security incidents efficiently.

Data Protection Policy

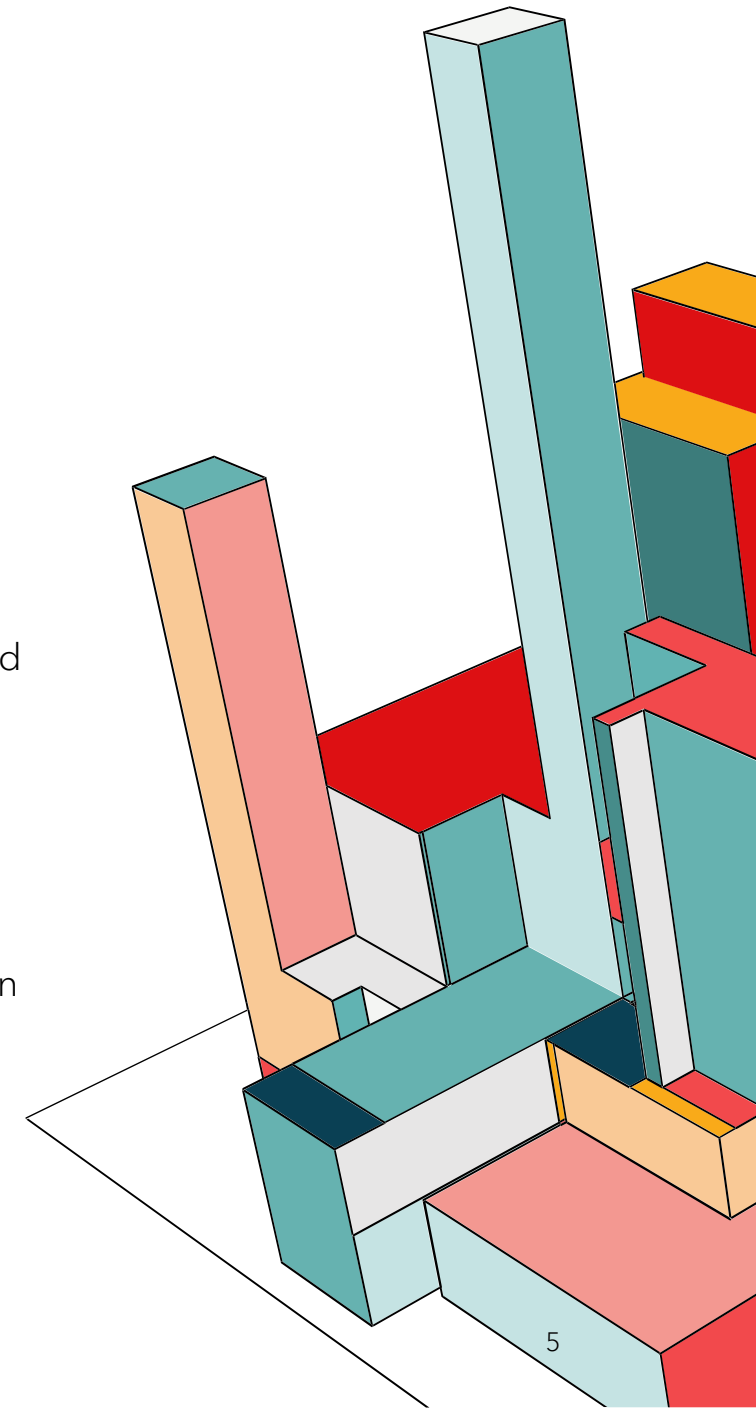
Ensures compliance with GDPR, PCI-DSS, and other regulatory standards to safeguard customer data.

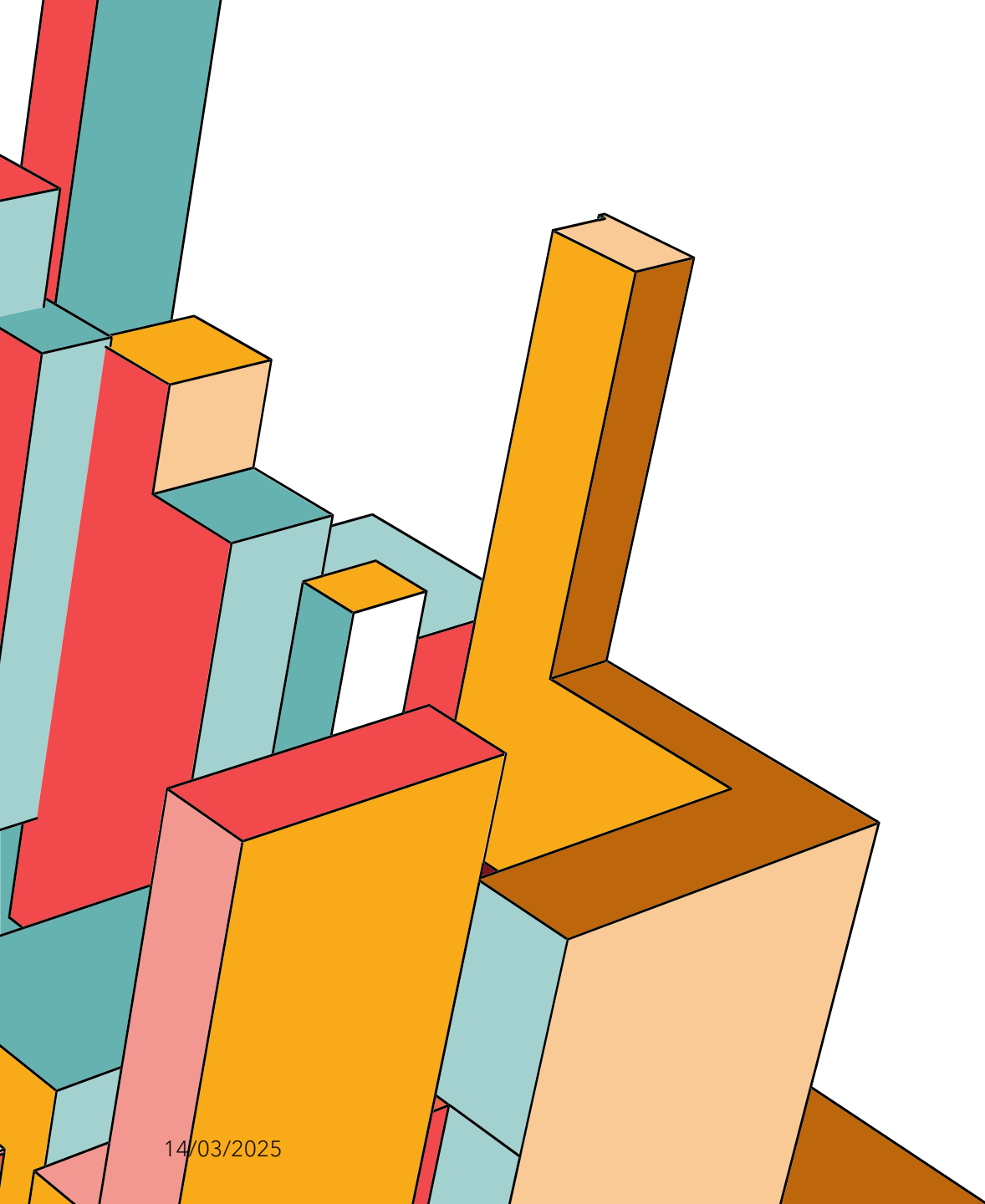
Vendor Risk Management

Requires third-party vendors to meet FSL's security requirements to prevent supply chain attacks.

BCDR Policy

Outlines steps to maintain operations and recover quickly in case of a cyberattack.





MITIGATION MEASURES

Technical Measures

Firewalls & Intrusion Prevention

Monitors and blocks malicious traffic before it reaches our internal network.

Multi-Factor Authentication (MFA)

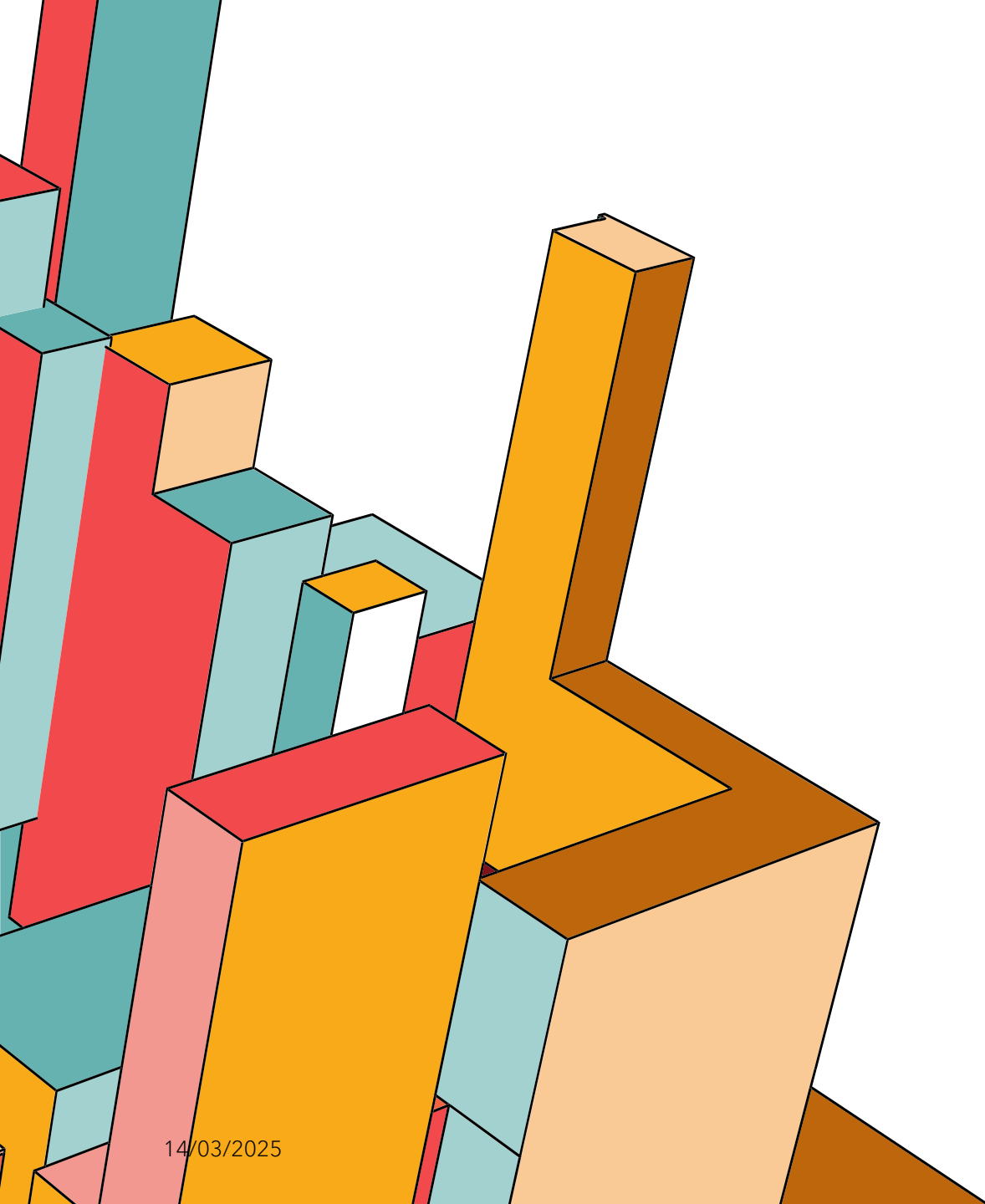
Adds extra layers of security beyond passwords, reducing unauthorized access risks.

Encryption & Endpoint Protection

Protects sensitive data both in transit and at rest, making it unreadable if intercepted.

Regular Patch Updates

Prevents attackers from exploiting outdated software vulnerabilities.



MITIGATION MEASURES

Administrative Measures

Background Checks

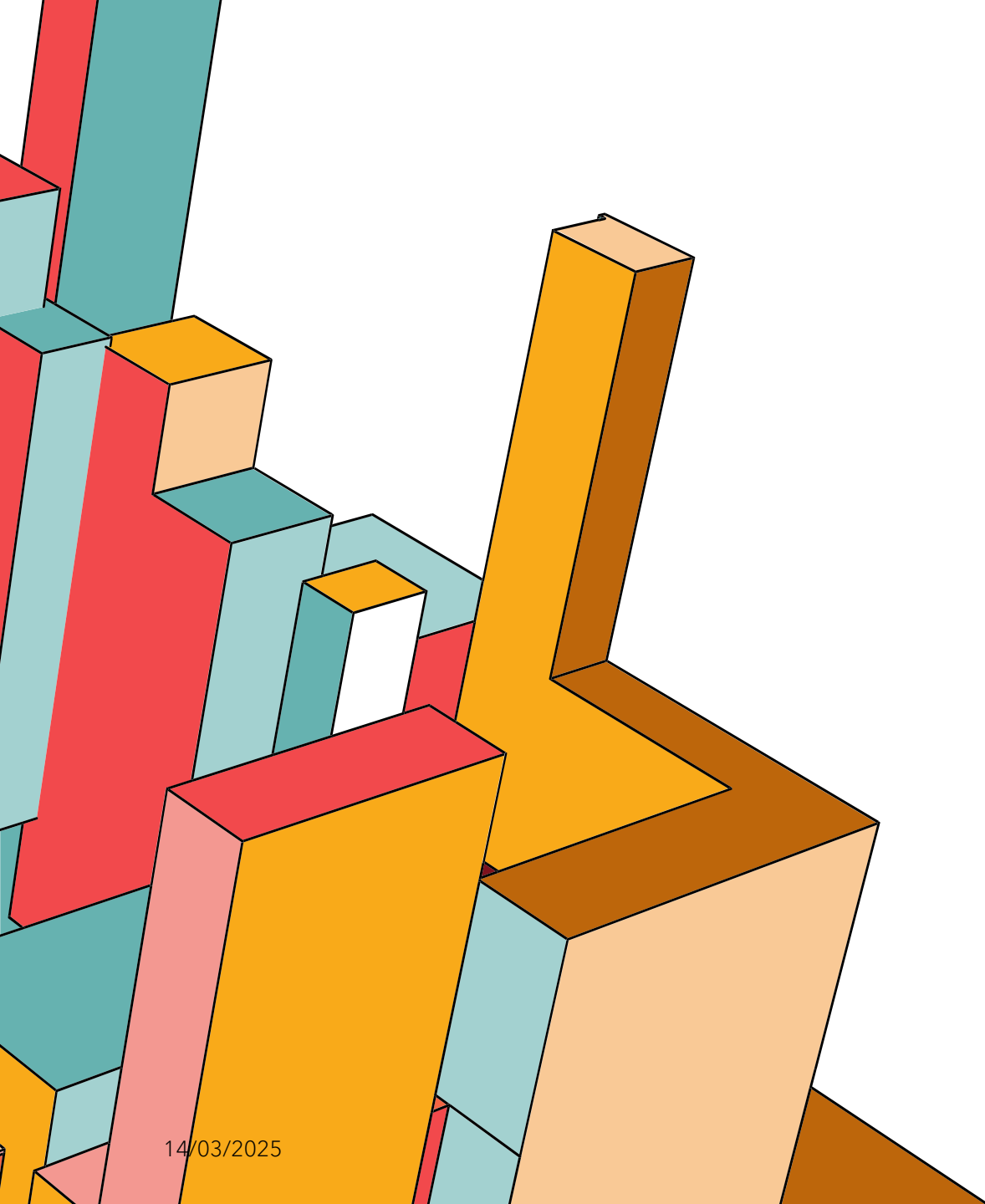
Screens employees before hiring to minimize insider threats.

Role-Based Access Control (RBAC)

Ensures employees only have access to the systems necessary for their job functions.

Vendor Security Audits

Regularly evaluates third-party vendors to ensure their cybersecurity measures align with ours.



MITIGATION MEASURES

Physical Security

Secure Facilities

Limits physical access to critical infrastructure using keycards, biometrics, and security guards.

Surveillance Systems

Monitors physical premises with cameras and access logs to detect and prevent unauthorized entry.

Controlled Access to Data Centres

Restricts who can enter sensitive IT environments, requiring biometric authentication or multi-factor access approval to prevent unauthorized physical tampering or insider threats.

MONITORING AND RESPONSE

Security Information & Event Management (SIEM)

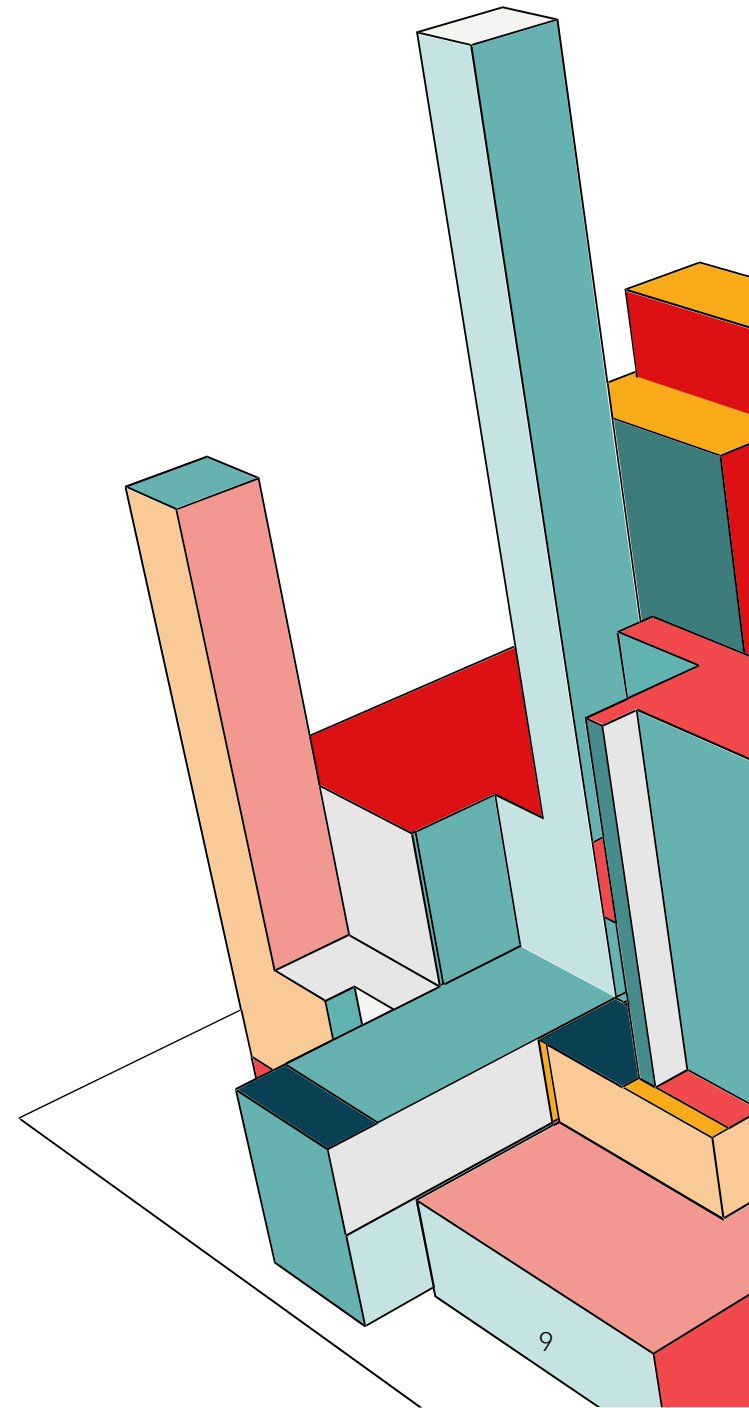
Analyzes security logs in real-time to detect anomalies and threats.

Incident Response Team (IRT)

A dedicated team trained to handle and mitigate security incidents quickly and efficiently.

Incident Response Plan (IRP)

A structured process for identifying, containing, and recovering from cybersecurity threats.



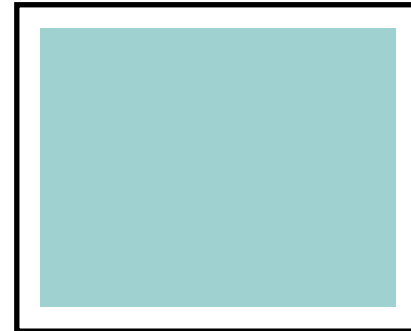
INCIDENT RESPONSE FLOWCHART

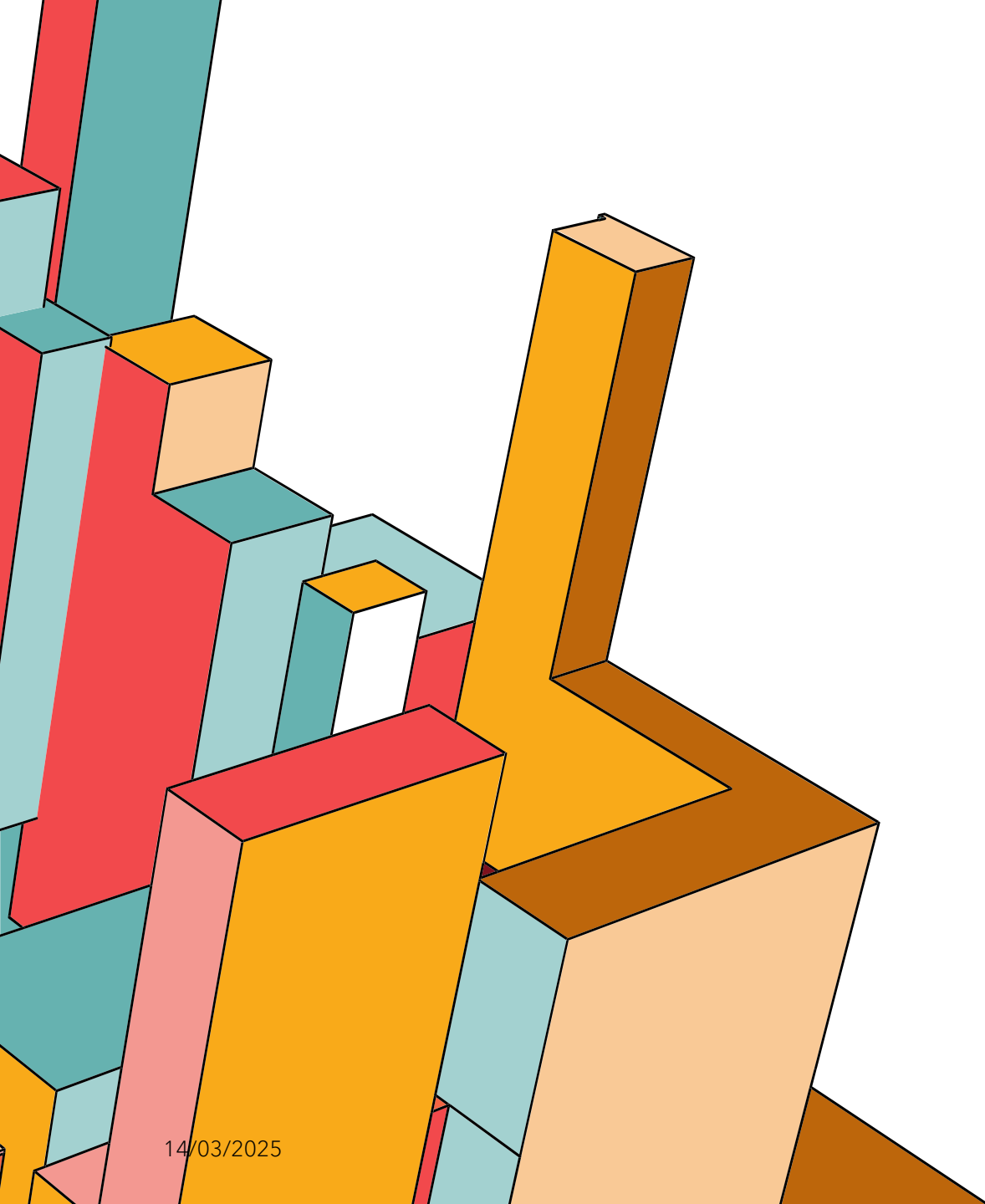


Threat Detected



Analyze Threat





EMPLOYEE TRAINING & AWARENESS

Regular Security Awareness Training

Educates employees on recognizing cyber threats and following security best practices.

Simulated Phishing Exercises

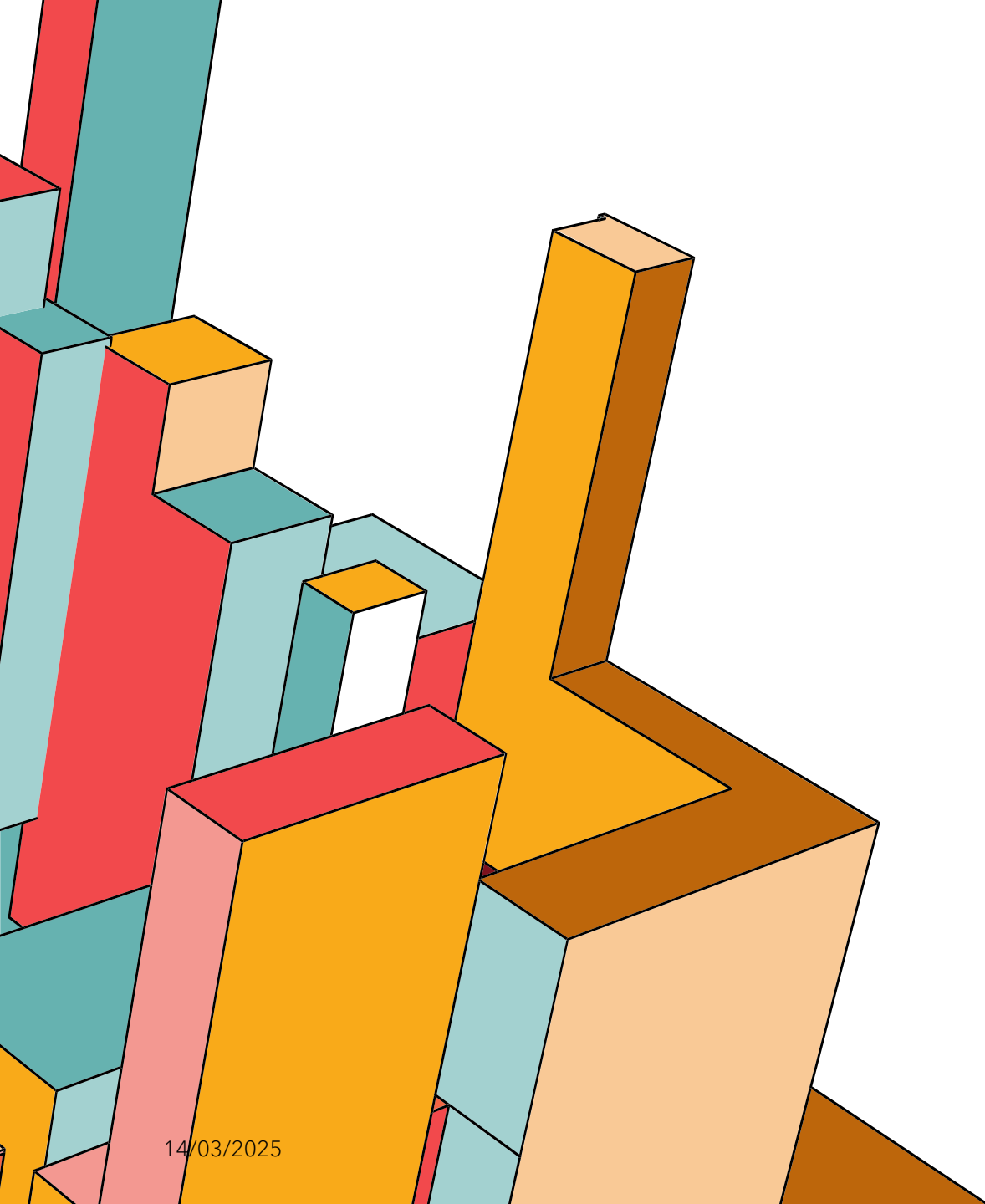
Tests employees by sending controlled phishing emails to improve their ability to detect threats.

Mandatory Policy Acknowledgment

Requires employees to confirm they understand and will comply with company security policies.

Role-Specific Training for High-Risk Departments

Tailored training programs for employees handling high-risk data and financial transactions.



EXPECTED BENEFITS OF IMPLEMENTATION

Stronger Security Posture

Reduces vulnerabilities and enhances protection against cyber threats.

Reduced Risk of Cyber Incidents

Proactive strategies lower the likelihood of breaches and data leaks.

Improved Compliance & Regulatory Alignment

Ensures FSL meets industry standards and avoids legal penalties.

Increased Customer Trust & Business Continuity

Demonstrates FSL's commitment to cybersecurity, strengthening customer confidence.

CONCLUSION & CALL TO ACTION

Implementing this strategy will
safeguard FSL's future

Approval and support from
leadership are crucial

Next steps: Formal adoption, budget
allocation, and phased implementation.

THANK YOU

Darius Moldoveanu

14/03/2025

2400622@student.uwtsd.ac.uk

University of Trinity Saint David's