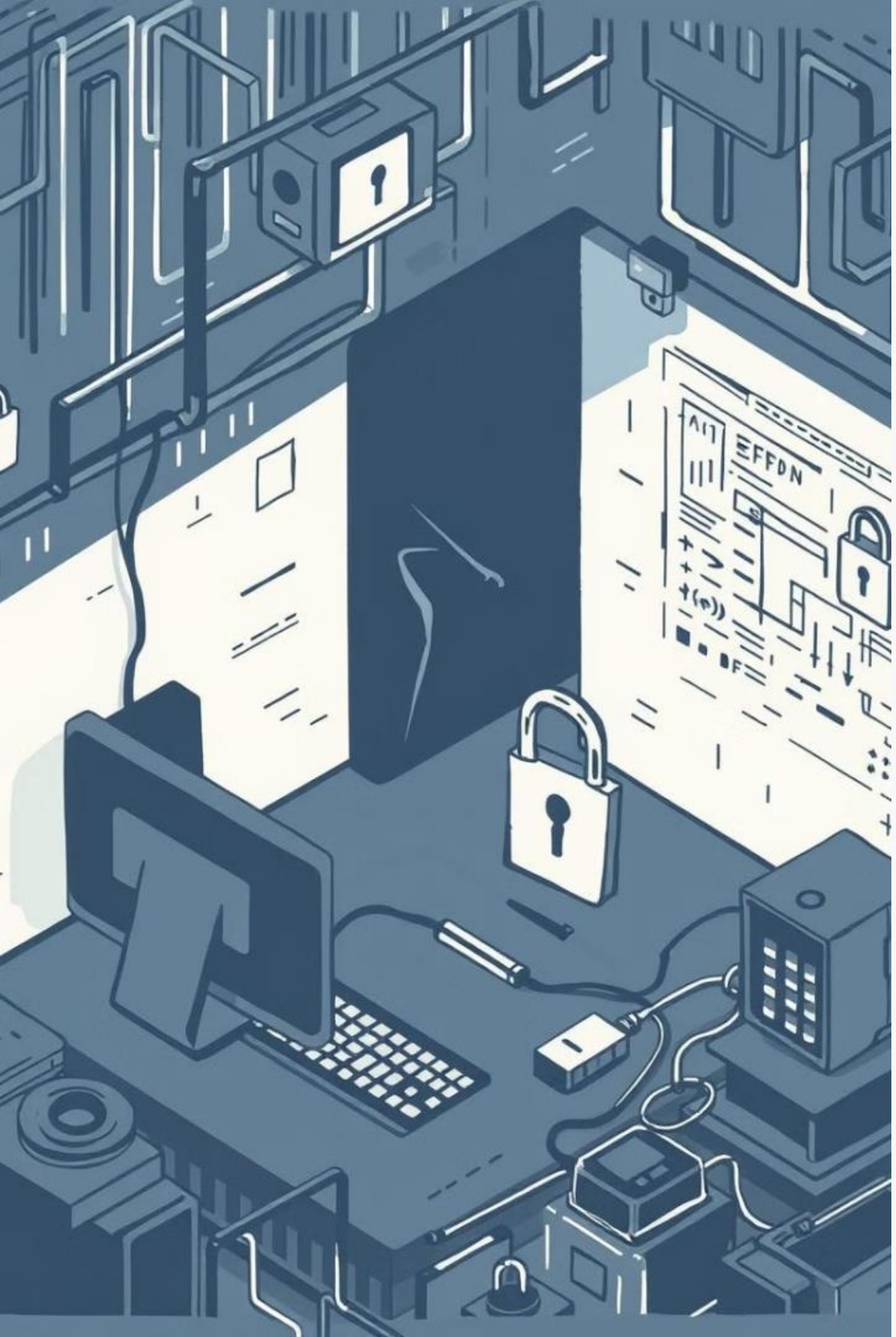


Cybersecurity Incident: Payment Scam Case Study

An accounts payable breach resulted in a $XX,000 AUD loss. This presentation will explore the details of the incident, the actions taken, and the lessons learned to prevent future occurrences.



Background

Our accounts payable specialists handle bills posting and weekly payment processing for the client X in the Northern Australia. Supplier "A" operates under an annual agreement with regular billing cycles (Yearly), with payments typically scheduled for Thursdays or Fridays.

Understanding these standard procedures is crucial for identifying deviations that signal potential security incidents. Any alterations to these established timelines should trigger immediate scrutiny and verification to prevent financial loss.

- Handling bills from Mailbox
- Bills Posting in MYOB
- Sending AP report for Payment approval

- Posting Payments In MYOB
- Generate ABA file

- Annual Agreement
- Payment with supplier A.

Incident Overview

The incident began on Tuesday with the receipt and posting of a bill. The aged payables report was sent for approval on Thursday. On Friday, payment entries were processed, and ABA files were saved. An urgent email, allegedly from Supplier "A," requested a bank detail update. The email appeared genuine, containing a thread of past conversations between the client and the supplier, updated the same after a quick review of the thread email. This incident led to the payment being processed to the altered information.

This timeline highlights the speed at which the scam unfolded, emphasizing the need for immediate verification of any changes to established payment processes.

1. Friday 10 AM
   Approved Aged Payables report received
2. Friday 12 PM
   Saved ABA files as payment deadline is at 1PM
3. Friday 12.30 PM
   Revised bill received with altered bank details



Discovery of the Scam

Two weeks later, Supplier "A" reported non-receipt of payment, triggering an investigation that revealed a **spoofed domain** (e.g., "@orangee.com.au" vs. "@orange.com.au"), altered bank details, and a manipulated email thread. The amount lost totaled $XX,000 AUD.

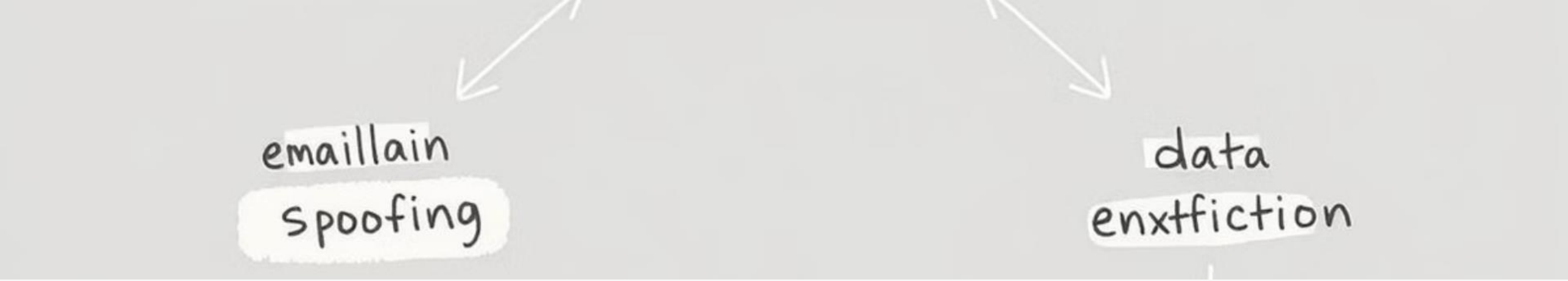
The discovery underscores the sophistication of the attack, where even minute details like domain names (single word change) were meticulously altered to deceive accounts payable staff.

Spoofed Domain

@orangee.com.au vs. @orange.com.au

Altered Details

Invoice Details were accurate.



Root Cause Analysis

The root causes included a sophisticated phishing attack involving the interception and manipulation of an ongoing conversation, domain spoofing where a minor alteration went unnoticed, and a process gap with no secondary verification for bank detail changes. The realistic replication of the email thread further contributed to the success of the scam.

1

Phishing Attack

Interception and manipulation of an ongoing conversation

2

Domain Spoofing

Minor alteration in the domain went unnoticed

3

Process Gap

No secondary verification for bank detail changes



Actions Taken Post-Incident

Following the incident, the client and supplier were immediately informed. Email headers were investigated for source tracking, and the scam was reported to relevant Australian authorities. Internal verification protocols were reviewed and revised to prevent future occurrences.

Swift action was crucial in mitigating further damage and initiating the recovery process, while also paving the way for implementing improved security measures.

1

Informed Parties

Informed client and supplier immediately

2

Investigated Email

Investigated email headers for source tracking

3

Reported Scam

Reported the scam to relevant Australian authorities

Lessons Learned

Key lessons included the need for stronger verification processes, the importance of domain awareness and scrutiny, the risks associated with email communication of sensitive details, and recognizing "urgency" as a common tactic used in phishing scams. These insights informed the subsequent improvements and preventive measures implemented.

These lessons serve as a foundation for building a more resilient and secure accounts payable process, capable of withstanding future attacks.

Stronger Verification

Need for stronger verification processes

Domain Awareness

Importance of domain awareness and scrutiny

Email Risks

Risks associated with email communication of sensitive details



Improvements Implemented

Improvements included cybersecurity enhancements such as Multi-Factor Authentication (MFA) for email accounts and advanced email filtering and anti-phishing software. Process changes involved dual verification for supplier bank detail changes and direct confirmation calls for sensitive requests. Staff training on identifying phishing and spoofed emails was also conducted.

These enhancements collectively strengthen the overall security posture of the accounts payable process, reducing the risk of falling victim to similar scams in the future.



Prevention Strategy & Future Measures

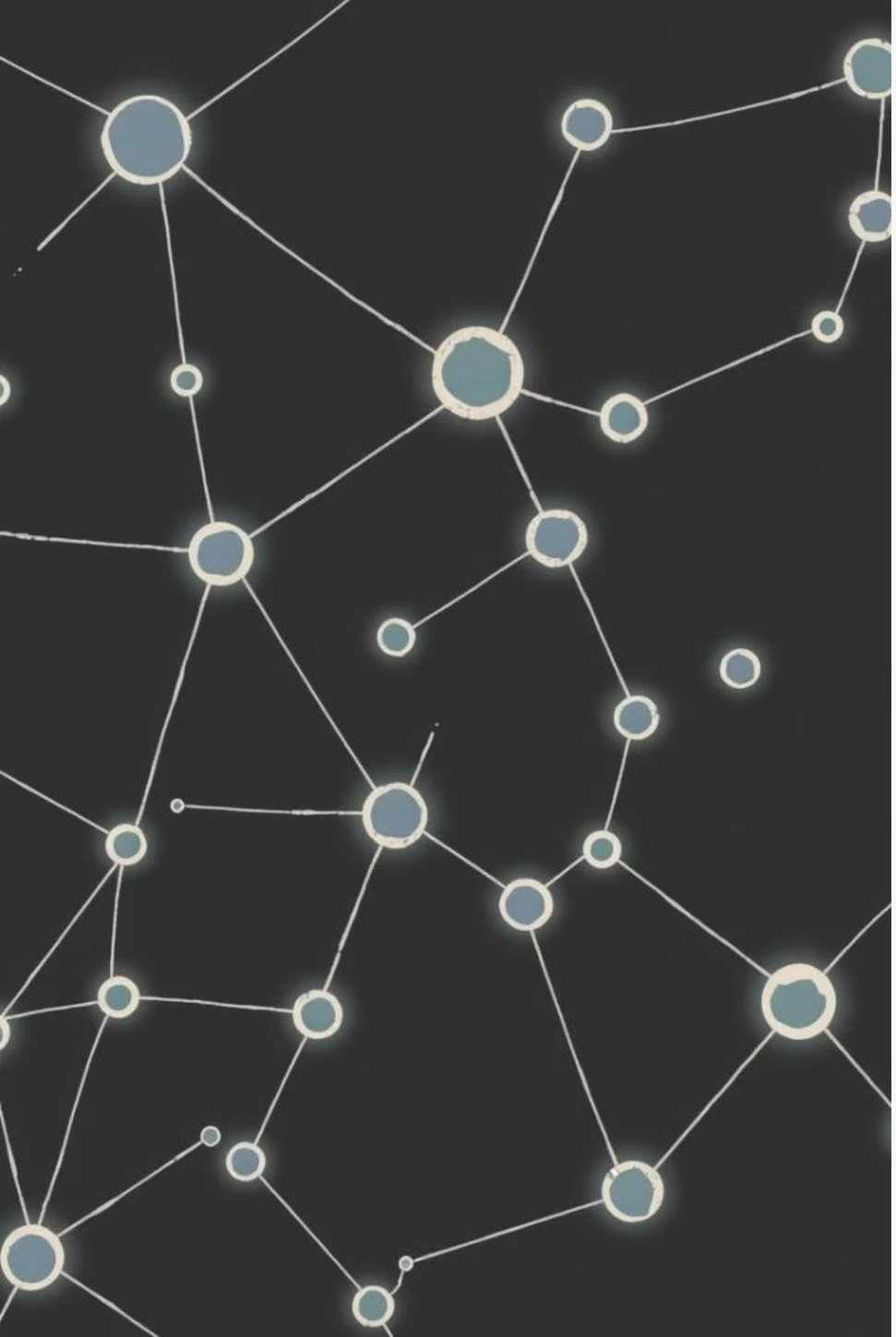
The prevention strategy includes mandatory checks of the bills before making payments and confirmation from Supplier contacts for the bank changes, if any, through email or through phone. Regular security audits of cybersecurity and payment protocols. Ongoing education on emerging phishing tactics and cyber attacks. These measures aim to create a proactive defense against evolving threats.

By continuously adapting and improving security measures, the organization can stay ahead of potential attackers and maintain the integrity of its financial processes.

1 Supplier Protocols

2 Regular Audits

3 Ongoing Education



Conclusion & Next Steps

In conclusion, the implemented measures have strengthened cybersecurity and verification processes while enhancing awareness and training to prevent future incidents. Ongoing collaboration with clients is essential for secure communication and maintaining a robust defense against evolving cyber threats. By staying vigilant and proactive, the organization can minimize its risk exposure and safeguard its financial assets.

The next steps involve continued monitoring, adaptation, and refinement of security protocols to ensure ongoing protection against future threats.