In many cases of Email compromise and Accounts Payable (AP) fraud, the victim may not know until after the money has left the country. Swift action can repatriate the funds and restore the victim organization, but time is of the essence. Well layered security and strong anti-fraud controls are important, but adversaries shift their tactics regularly and often find ways to attack unexpectedly. At Protiviti, we build on a foundation of strong business process and security advisory services, but we also bring the ability to react to new and evolving threat actors.

Protiviti’s Cyber Threat Intelligence labs constantly analyze data from our Incident Response Teams in the field and enrich it with context from threat feeds, Dark Web research, and our threat intelligence network peers and vendors. We apply this knowledge to fraud prevention, security awareness training, detective controls, and reactive controls advisory. We supplement or client’s capabilities and deliver confidence to their reactions to challenges form the threat environment.

<table>
<thead>
<tr>
<th>User re-uses credentials on web sites</th>
<th>Attacker finds credentials</th>
<th>Attacker accesses cloud mail</th>
<th>Attacker impersonates AP supervisor</th>
<th>AP Clerk initiates ACH to Treasury</th>
<th>Treasury approves</th>
<th>Bank issues ACH</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1.png" alt="User re-uses credentials" /></td>
<td><img src="image2.png" alt="Attacker finds credentials" /></td>
<td><img src="image3.png" alt="Attacker accesses cloud mail" /></td>
<td><img src="image4.png" alt="Attacker impersonates AP supervisor" /></td>
<td><img src="image5.png" alt="AP Clerk initiates ACH to Treasury" /></td>
<td><img src="image6.png" alt="Treasury approves" /></td>
<td><img src="image7.png" alt="Bank issues ACH" /></td>
</tr>
</tbody>
</table>

Where could we have stopped it?

- Security Awareness Training
- Cyber Threat Intelligence
- Multi-Factor Authentication
- Separation of Duties Controls
- ERP Coordinated with Treasury
- Separation of Duties
- Incident Response
- Law Enforcement
- SWIFT
- Call back from Bank

The attacker is evolving and so can you. Combine business process improvements, fraud prevention, cyber security, and the capability to react swiftly to build organizational resilience to evolving attacks.
1. Recover the Funds
   • Contact counsel as soon as possible after discovering the fraud. Counsel can contact the appropriate law enforcement entity.
   • Contact the bank. The SWIFT network can be used to recover or impound the funds. International actions may require aid from law enforcement.
   • Contact your fraud & forensic vendor.

2. Gather Information
   • Gather as many details as possible while memories are fresh.
   • Was there collusion or negligence? Regulators, Auditors, Boards of Directors, and others may ask. Be able to Answer with Confidence.
   • A root cause technology analysis combined with a fraud investigation provide the answers you need and recommendations.

3. Immediate Protection
   • Place your Accounts payable functions and Treasury functions on alert and scrutinize irregular requests.
   • Many attackers make multiple attempts at fraud and many are successful.
   • Most fraud involves new ACH or Wire details. Scrutinize and confirm such changes until long-term improvements can be made.

4. Enduring Protection
   • Multi-factor authentication is a must for any system connected to the Internet, like cloud mail services.
   • Review Email systems and consider Email proxy services that help identify malicious and misleading content.
   • Review policies and assess compliance for cash movement.

5. Breed Resilience to this Threat
   • Build a Culture of Compliance within your organization through simulations and engaging security awareness training.
   • Train VIP’s with engaging and customized programs to avoid targeted fraud called spear phishing.
   • Identify key people and positions “XIP’s” in the chain of events leading to fraud. Provide customized prevention training.

6. Remediation
   • Use business process to build resilience. Consider automating ERP and Treasury verifications and blocking suspicious acts.
   • Implement leading practices in separation of duties and encourage compliance with fraud prevention efforts.
   • The attacker is evolving to adapt to security and process improvements, stay up with the latest developments.

Schedule a call with our digital forensic and incident response experts today by contacting us at IR@Protiviti.com.