**Impacts:**

Both whaling and Business Email Compromise attacks can have significant political and economic consequences. Commercial whaling has led to international disputes and strained diplomatic relations, while BEC attacks cause direct financial losses and reputational damage to businesses, Impacting economic stability and investor confidence.

**Whaling‘s Political, Social and Economic Impacts:**

**Policy manipulation:**

Hackers may get knowledge about election strategies or policymaking, giving them the ability to influence political outcomes or spread misleading information. Political scandals, such as the intervention in the 2016 U.S. election, could result from whaling attacks that target top officials or campaign managers and cause emails to leak.

**Economic Impacts:**

Businesses lose millions of dollars as a result of unauthorized wire transfers.   
Attackers may pretend to be a CEO who requests payment right away. For example, a CFO could be tricked into sending funds to a fraudulent account, which could result in a large loss and problems with an audit.

**Loss of Public Trust:**

Client and Publicly revealing a whaling attack can erode customer and staff trust, especially when private data is involved. For instance, patient records may be jeopardized when a hospital CEO is picked out by whaling, causing privacy concerns and public outrage.

**BEC Attacks’ Political, Social and Economic Impacts:**

**Financial losses:**

BEC attacks, where cybercriminals impersonate trusted individuals to defraud organizations, can result in massive financial losses for businesses. These losses can range from stolen funds to compromised data, impacting a company’s ability to operate and invest. Example Toyota Boshoku Corporation lost $37 million due to a BEC attack that tricked an employee into changing bank account information.

**Reputational Damage:**

Successfully executed BEC attacks can severely damage a company’s reputation, leading to a loss of customer trust and investor confidence. Example A BEC attack targeting Google and Facebook resulted in a $121 million loss after attackers impersonated a legitimate vendor.

**Economic instability:**

Large –scale BEC attacks can destabilize entire industries or even economies, especially if they target critical infrastructure or financial institutions. Example A construction company anticipating a large payment for a project might receive an email from a seemingly legitimate vendor requesting a change in a payment details for the next installment. The email could include a slightly different bank account number and a sense of urgency due to upcoming deadlines. The employee, under pressure to meet deadlines and avoid potential delays, might not verify the details and make the payment to the fraudulent account.

**Legal implications:**

BEC attacks can lead to legal battles and financial penalties for the affected organizations, further impacting their economic stability. Example The FBI’s Internet Crime Complaint Center (IC3) reported billions of dollars lost due to BEC attacks in 2019, highlighting the scale of the problem.

**Security measures:**

**Email Security:**

Employing email filtering software to block suspicious emails, implementing two-factor authentication (2FA) for emails accounts and using email security protocols like SSL/TLS, SPF, DMARC and end-to-end encryption. In Multi –Factor Authentication (MFA), adds an extra layer of security to email accounts beyond just password. It requires users to provide two or more verification factors to login, making it significantly harder for unauthorized users to gain access.

**Employee Training:**

Educating employees on how to recognize whaling and BEC attacks, including phishing attempts, and providing regular security training to maintain awareness. Also reporting suspicious Emails to the IT or security team for investigation.

**Verification process:**

Implementing strong verification processes for financial transactions, such as confirming requests through multiple channels and establishing clear communication protocols. Employee can be trained to examine email headers for inconsistencies or suspicious information, especial if an email contains attachment from an unknown sender.

**IT infrastructure:**

Ensuring a properly configured and managed IT infrastructure, including regular software updates and threat monitoring is crucial. Firewall acts as barrier between the internal network and external networks, controlling network traffic and preventing unauthorized access. Final IDS/IPS are network malicious that can automatically block threat.

**Password Policies:**

Enforcing strong password policies, including using password managers and continuously scanning endpoints for vulnerability. Should also address password recovery and the secure storage of recovery information.