BUSINESS EMAIL COMPROMISE

STAYING AHEAD OF THE THREAT WITH EFFECTIVE PREVENTION AND RESPONSE

Presented by Texas Association of Counties

12/1/2023

DISCLAIMER

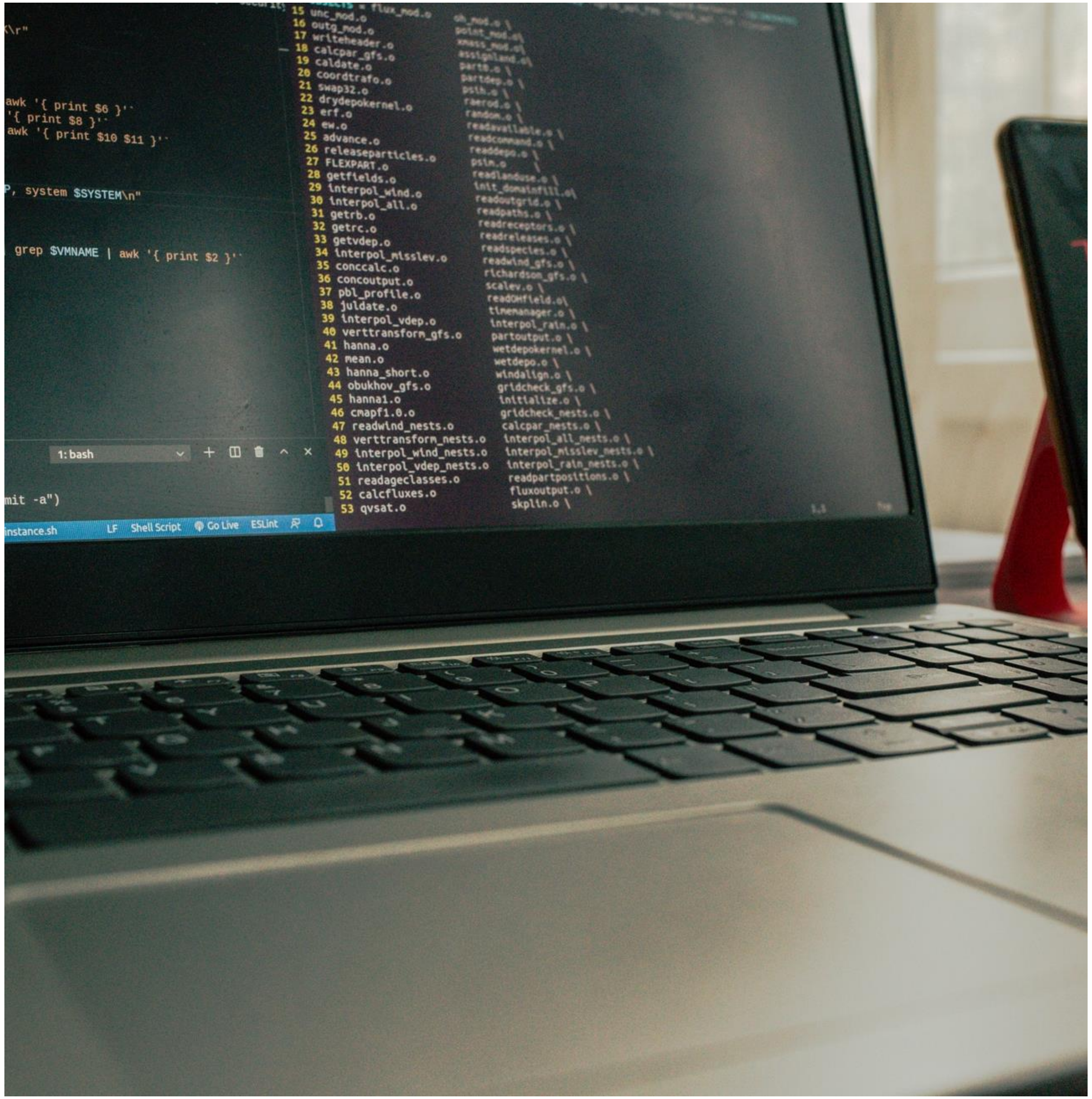
The information presented in this session is for educational purposes only. Possible claim scenarios discussed are hypothetical and are not official coverage determinations. Coverage as provided by TAC Risk Management Pool is subject to the terms and conditions of the specific coverage document.

Items presented are best practices only and are not a requirement of TAC RMP coverage. TAC is not endorsing any software, services, or technology companies when referenced in this presentation.

This training does not satisfy or comply with HB3834 (86th Legislature) or any state statute requiring cybersecurity training.

WHAT IS BEC?

Business Email Compromise (BEC) is a type of cybercrime that targets local government, businesses, and organizations. It involves attackers compromising legitimate business email accounts and using them to request fraudulent wire transfers or other sensitive information.



THREAT ACTORS

Who is launching the attacks and why

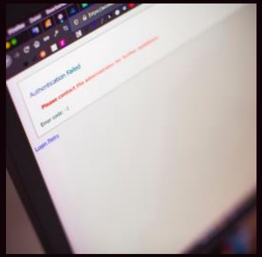
Hacktivism

Criminals

Nation States

Insider Threats

Opportunistic



User Error

TYPES OF BEC ATTACKS

False Invoice Scam: In this attack, the phisher pretends to be a vendor requesting payment for services performed for the company. Often, this type of attack will masquerade as one of an organization’s actual suppliers and use a realistic template but change the bank account information to an account controlled by the attackers.

CEO Fraud: CEO fraud takes advantage of power dynamics within a company. The attacker will send an email – supposedly from the CEO – instructing the recipient to take some action. This may be to make a wire transfer to “close a business deal” or sending sensitive information to a partner.

Account Compromise: An account compromise BEC attack takes advantage of a compromised email account within an organization. With this access, the attacker can request invoice payments from customers while changing the payment details to those of the attacker.

Attorney Impersonation: This type of attack takes advantage of the fact that low-level employees within an organization are likely to comply with requests from a lawyer or legal representative because they don’t know how to validate the request. This approach often makes the request seem time-sensitive and confidential to prevent independent verification.

REAL TEXAS EXAMPLES

2023 - Large Panhandle County - Fake invoice - $566k

2022 - TAC Members - 2/3 cyber claims have BEC events involvement

2019 - Smaller County Jail - Phishing email from personal account led to Ransomware

SECURE NETWORK MONITORING AND LOGGING SOLUTIONS (NMLS)

DISASTER RECOVERY PLANS AND PROCEDURES (DRPP)

SECURE IDENTITY AND ACCESS MANAGEMENT (IAM) DATA PROTECTION REGULATIONS AND REQUIREMENTS (DPRRS) INTRUSION DETECTION SYSTEMS

SECURE APPLICATION FIREWALLS (AFW) IT GOVERNANCE POLICIES AND PROCEDURES (ITGPS) SECURE CLOUD DATA LOSS PREVENTION SOLUTIONS (CDLP)

SECURE CLOUD MONITORING AND LOGGING SOLUTIONS (CMLS) IT RISK MANAGEMENT POLICIES AND PROCEDURES (ITRMPS) SECURE CLOUD ENCRYPTION SOLUTIONS (CES)

PENETRATION TESTING

SECURE ENDPOINT PROTECTION PLATFORMS (EPP)

SECURE APPLICATION SECURITY TESTING (AST)

FRAUDULENT TRANSACTIONS

SECURITY AUDITS

SECURE NETWORK ACCESS CONTROL SYSTEMS

SECURE EMAIL GATEWAYS ENDPOINT SECURITY

DATA ENCRYPTION BEC COST CYBER ATTACK

CLOUD SECURITY SOLUTIONS

SECURE WEB GATEWAYS

MALWARE DATA BREACH FINANCIAL LOSSES

NETWORK SECURITY

URE WEB APPLICATION FIREWALLS

ECURE DATA LOSS PREVENTION (DLP)

URE FILE SHARING SOLUTIONS (SFSS)

E NETWORK ACCESS CONTROL (NAC)

PHISHING RANSOMWARE FIREWALL PROTECTION

ECURE REMOTE ACCESS SOLUTIONS

IDENTITY THEFT SECURITY SOLUTIONS

PASSWORD PROTECTION CYBERSECURITY DATA LOSS PREVENTION

DATA PRIVACY REGULATIONS AND REQUIREMENTS (DPRRS)

REGULATORY COMPLIANCE REQUIREMENTS (RCRS)

COMPLIANCE MANAGEMENT PROGRAMS (CMPS)

BUSINESS CONTINUITY PLANS AND PROCEDURES (BCPP)

SMALL BUSINESSES

VENDOR RISK MANAGEMENT PROGRAMS (VRMP)

INCIDENT RESPONSE PLANS AND PROCEDURES (IRPP)

SECURE CLOUD BACKUP AND RECOVERY SOLUTIONS (CBRS

SECURE CLOUD SECURITY SOLUTIONS (CSS)

BUSINESS EMAIL COMPROMISE

SECURE APPLICATION WHITELISTING (AWL)

SECURE FILE TRANSFER PROTOCOLS (SFTP)

VULNERABILITY SCANNING

SECURE DATABASE SECURITY SOLUTIONS (DSS) MULTI-FACTOR AUTHENTICATION SECURE CLOUD ACCESS SECURITY BROKERS (CASB)

SECURE MOBILE DEVICE MANAGEMENT SOLUTIONS

INFORMATION SECURITY POLICIES AND PROCEDURES (ISPPS) SECURE CLOUD INFRASTRUCTURE SECURITY SOLUTIONS (CISS)

SECURE ENDPOINT DETECTION AND RESPONSE (EDR) THIRD-PARTY RISK MANAGEMENT PROGRAMS (TPRM)

SECURITY AWARENESS TRAINING PROGRAMS (SATP)

SECURE CLOUD IDENTITY AND ACCESS MANAGEMENT SOLUTIONS (CIAM)

SECURE NETWORK INTRUSION PREVENTION SYSTEMS (NIPS)

STEPS TO PREVENT BUSINESS EMAIL COMPROMISE

Train Employees

Educate employees on the risks of BEC and how to identify suspicious emails.

Implement Security Policies

Ensure that all employees are following security protocols and policies.

Monitor Email Traffic

Monitor email traffic for suspicious activity.

PREVENTION

1

Awareness Training

Cybersecurity Workshops

Regular newsletter

Phishing training/testing

2

Strong Passwords/MFA

Strong & Unique Passwords

Regularly changed

Multi-Factor Authentication

3

Develop Policies and SOPs

Have SOPs to clearly define roles

Policies about: Email use, Social Media, Acceptable Use, etc.

4

Stay Informed & Vigilant

Know what's going on in other counties, vendors, and other entities

What's new in the county

RESPONSE

- When an incident happens…

  What process or policies do you have to follow?

  What is the reporting process and who?

  Call TAC Risk Management Pool - your Cyber Coverage provider

- Have a playbook

  Have an easily accessible document or handout to refernce

  Define the roles and responsibilities of those impacted by the incident

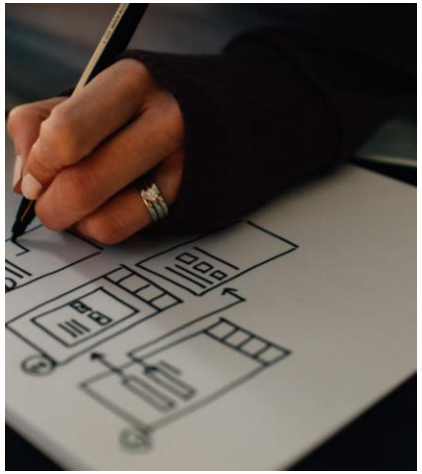
  Develop a path for communication of incident to county

- Who's in charge of communication?

  Who is the IT person in charge?

  Who handles the claim?

  What about media, inter-office, public, etc?



RESOURCES

- Stop. Think. Click.
  https://stopthinkclick.org/
- Cybersecurity & Insfrastructure Security Agency
  https://cisa.gov/
- TX Dept. of Information Resources
  https://dir.texas.gov/
- eRiskHub
  https://eriskhub.com/
- Texas Association of Counties - RMP
  https://county.org
- Peers

THANK YOU

Brandon Armstrong

Cybersecurity Risk Consultant

BrandonA@county.org

cell: 210-773-6045

Texas Association of Counties