Business Guide: Cybersecurity Awareness

CAPE COD 5

5 QUICK TAKEAWAYS

1. **Train your staff** on information security procedures and phishing awareness. Repeat often.
2. **Work with an IT resource** to keep your computer systems up to date and your network secure.
3. **Utilize the Treasury Management Services** your bank offers as part of your strategy to prevent unauthorized access to your financial accounts. Ask your bank about services such as dual control, positive pay and ACH debit block. Verify all payment requests using contact information you have on file, not the contact information included with the instructions.
4. **Take inventory of all the vendors** you do business with and where your sensitive information is stored – get comfortable with the controls they use to protect your data.
5. **Document an incident response plan now** – how you will respond to and recover from a cyber event and who you need to help you. Regularly back up data. Consider cyber insurance.

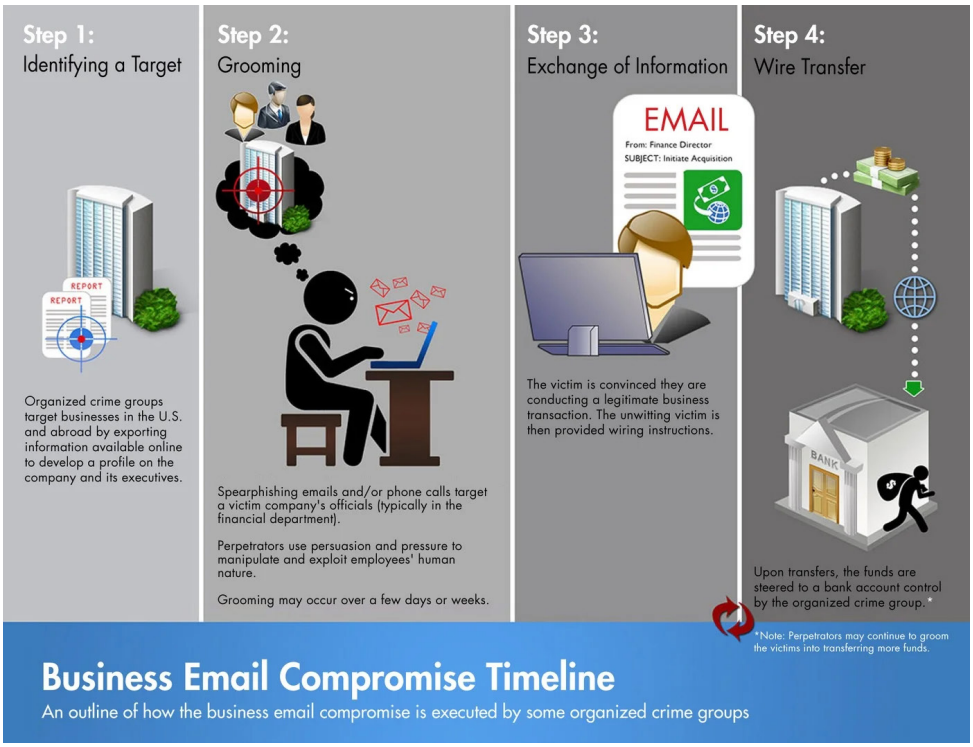
Threat Environment

By the Numbers

- According to FBI data, more than **$55 billion dollars** in losses were suffered due to Business Email Compromises (BEC) in the last ten years (2013-2023).
- In 2023, the Federal Trade Commission (FTC) received over 330,000 reports of business impersonation scams, which is the most reported type of fraud. Reported losses from these scams? **> $1.1 billion**
- According to the 2023 Association for Financial Professionals Survey Report, **63% of businesses reported experiencing check fraud in 2022.**
- Financial Crimes Enforcement Network (FinCEN) found that more than **$688 million** in check fraud linked to mail theft was reported over a six-month period in 2023.

Cyber Attacks: The "How"

- Criminals target victims through social engineering campaigns such as phishing, which leaves you and your employees victim to BEC and other credential harvesting opportunities.
- Criminals also access dark web databases that sell credentials from historical data breaches.
- Criminals compromise your credentials to log into your system, deploy malware and takeover your account.
- Outdated software and missing patches can expose vulnerabilities to your current operating systems, making your network more susceptible to an attack.



Credit: FBI IC3 Advisory

Key Considerations for Your Information Security Program

- **Require strong passwords for all devices** - at least 12 characters that are a mix of numbers, symbols and capital/lowercase letters. No "dictionary" words. Use unique passwords for every application and require your employees to change them regularly. Never allow password sharing.
- **Use Multi-Factor Authentication (MFA)** - this "steps up" security by requiring something more than a password, like a temporary code or a hard token that is inserted into your device, to access your account.
- **Regularly back up data.** Know where your data is stored and how it is protected. Encrypt data at rest and in transit (for example, use a secure email program for sending sensitive files).
- **Limit access.** Create tiered rights for employees based on job function. Sometimes the threat is internal, not external – require dual control for higher risk transactions.
- **Require employees to do personal business on their own devices**, not on business computers (if an employee clicks a malicious hyperlink in their personal email, it could impact the entire network).
- **Do not allow employees to download/ install computer programs** without an established review protocol. Do not allow "thumb drives" or other removable media on your computer network.
- **Document how to safely dispose** of physical and electronic files and old devices/hardware.
- **Train staff on these information security procedures**, including the cost of non-compliance: money and reputation.
- **Include any third parties/vendors** with access to your data as part of your information security plan. If they have a breach, that could have major implications for your business.

Krebs's 3 Rules for Computer Safety

1. If you didn't go looking for it, don't install it.
2. If you installed it, update it.
3. If you no longer need it, get rid of it.

(Brian Krebs – Krebsonsecurity.com)

How to Respond to an Incident

Contain → Eradicate → Recover → Notify → Review

Contain: Limit the damage. If compromised, disconnect infected devices from your network. Notify financial institutions to protect bank accounts.

Eradicate: Professionally clean compromised devices.

Recover: Restore data from back-ups.

Notify: Make law enforcement aware – local and FBI Internet Crime Complaint Center (IC3). Notify staff and customers. Notify your financial institutions if your online account access was potentially compromised.

Review: Look at existing controls and make modifications as necessary. Retrain staff.

Resources

- Federal Trade Commission (FTC): Cybersecurity for Small Business www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity
- FTC Data Breach Response: A Guide for Business: www.ftc.gov/data-breach-resources
- FBI Internet Crime Complaint Center (IC3): www.ic3.gov
- National Institute of Standards and Technology (NIST): https://www.nist.gov