oswald

GBQ

Combating Business Email Compromise - Don’t Be The Next Victim

August 25, 2020

Agenda

- Business Email Compromise Defined
- Business Email Compromise Impacts
- Responding to the Breach
- Preventing Business Email Compromise at the left of the breach

Speakers

Doug Davidson
Director of Information Technology Services
GBQ
(614) 947-5340
ddavidson@gbq.com

Jeremy Bronson
Director, Accounting & Business Advisory Services
GBQ
(419) 885-8338
jbronson@gbq.com

Lacy Rex
Vice President, Cyber Strategic Leader
Oswald Companies
(513) 716-6002
lrex@oswaldcompanies.com

Michael Casey
Vice President, Market Leader, Toledo
Oswald Companies
(567) 200-2572
mcasey@oswaldcompanies.com

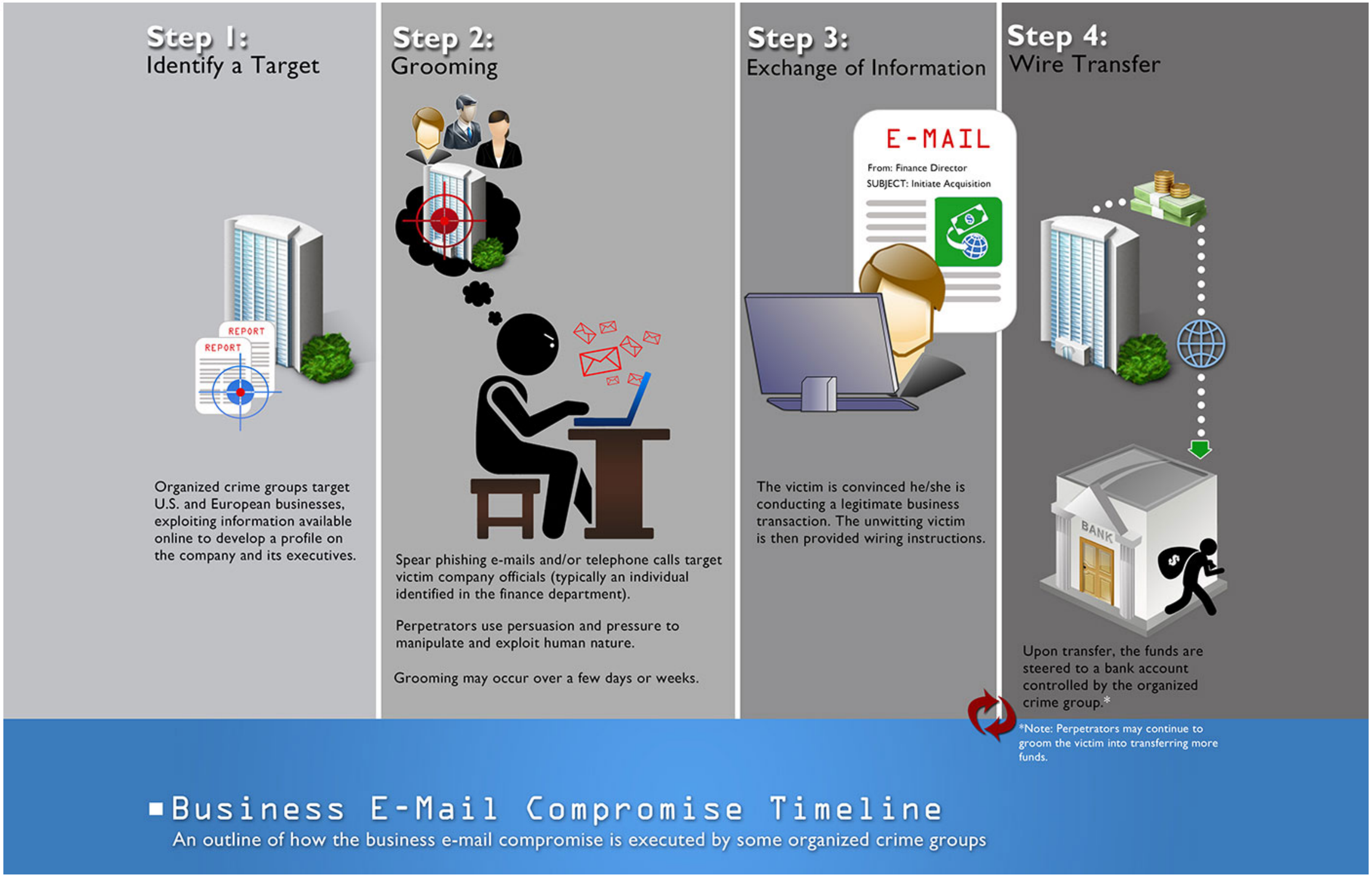
Welcome

- **Tremendous Effort to Suddenly Implement Remote Infrastructure**
  - Did more with less
  - Did it with great speed

- **Workers Remain the Weakest Link in the Corporate Security Chain**
  - New infrastructure leaves them further exposed
  - Attack patterns showing hacker awareness of weaknesses

- **Business Email Compromise - not new, but growing**
  - Companies moved to Office 365 to support work from home
  - 2020 is a tough enough business environment without adding a loss event
  - GBQ's IT services is responding to an increased number of these events

Business Email Compromise



Step 1: Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2: Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3: Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4: Wire Transfer

Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

- Business E-Mail Compromise Timeline

An outline of how the business e-mail compromise is executed by some organized crime groups

Source: https://www.fbi.gov/news/stories/business-e-mail-compromise-on-the-rise

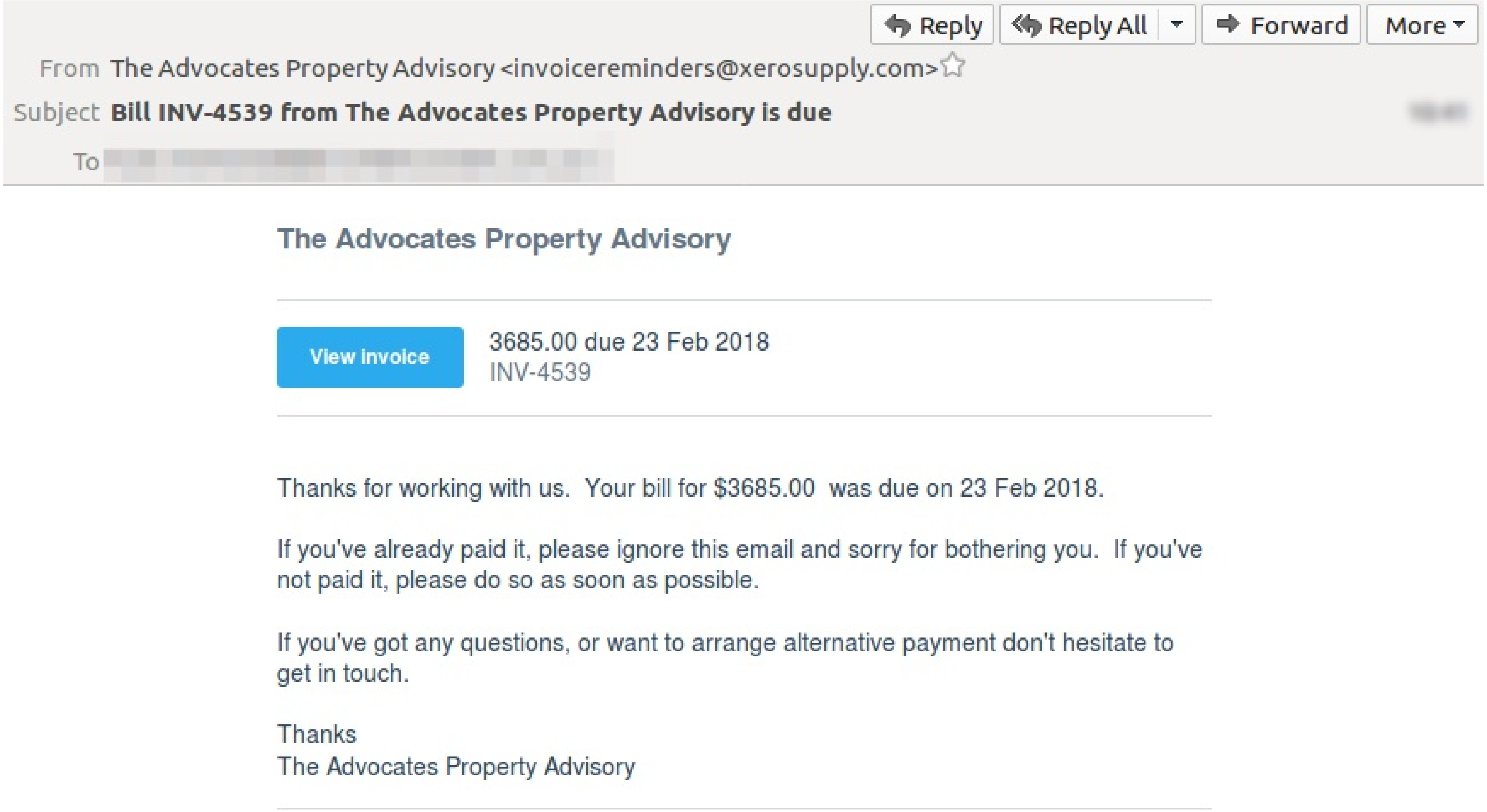
Characteristics of BEC

- Often there is no payload – user & internal controls are last line of defense, NOT technology safeguards
- Low volume email targeting, high value individuals
- Personalized from publicly available information
- Few to no ‘traditional’ spam/phishing tells (such as poor grammar, egregious misspellings, etc.)
- Sometimes attacks come from legitimate contacts who have lost control of their email systems

Common BEC Scenarios

Fake Invoice Scheme	CEO Fraud	Account Compromise	Attorney Impersonation	Data Theft
Attackers issue a fraudulent invoice, usually impersonating a foreign supplier sometimes from the suppliers email	Attackers pretend to be a company executive and demand an urgent wire transfer, data transfer, gift card or something else of value.	Attacker hacks an employee email account and requests payments from vendors or an internal payment.	Attackers impersonate a lawyer or other official (e.g. payroll service, etc.) who handles confidential information, and requests more sensitive data from staff.	Attackers target HR and accounting employees to steal sensitive data, including tax information. Data sometimes used in future BEC attacks or is monetized in its own right.

BEC in Action – Real World Example



From The Advocates Property Advisory <invoicereminders@xerosupply.com>

Subject **Bill INV-4539 from The Advocates Property Advisory is due** [redacted]

To [redacted]

The Advocates Property Advisory

3685.00 due 23 Feb 2018
INV-4539

Thanks for working with us. Your bill for $3685.00 was due on 23 Feb 2018.

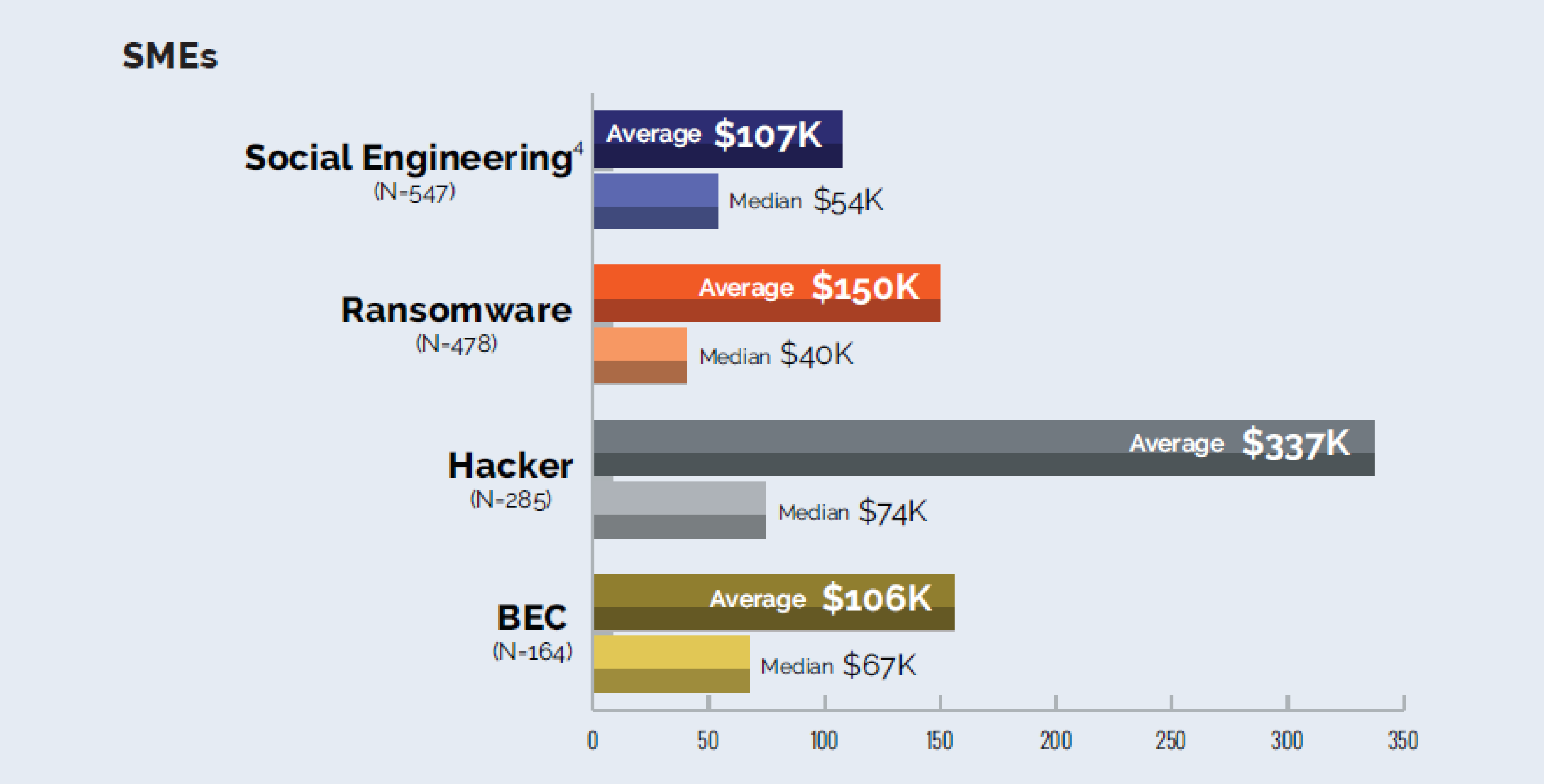
If you've already paid it, please ignore this email and sorry for bothering you. If you've not paid it, please do so as soon as possible.

If you've got any questions, or want to arrange alternative payment don't hesitate to get in touch.

Thanks
The Advocates Property Advisory

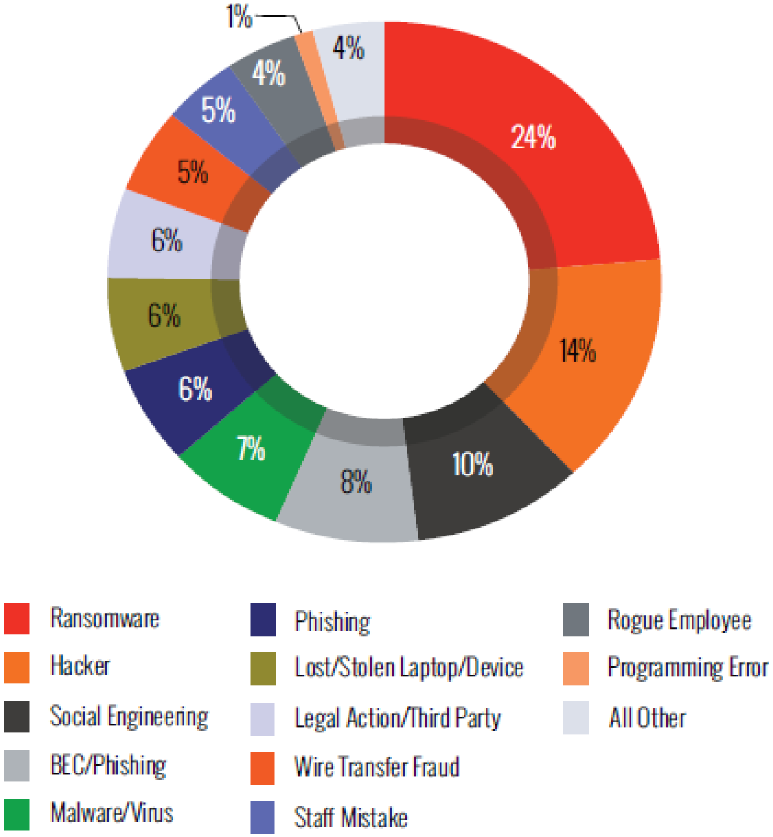
Who Are the Attackers?

Cause of Loss for SMEs (Under $2B)

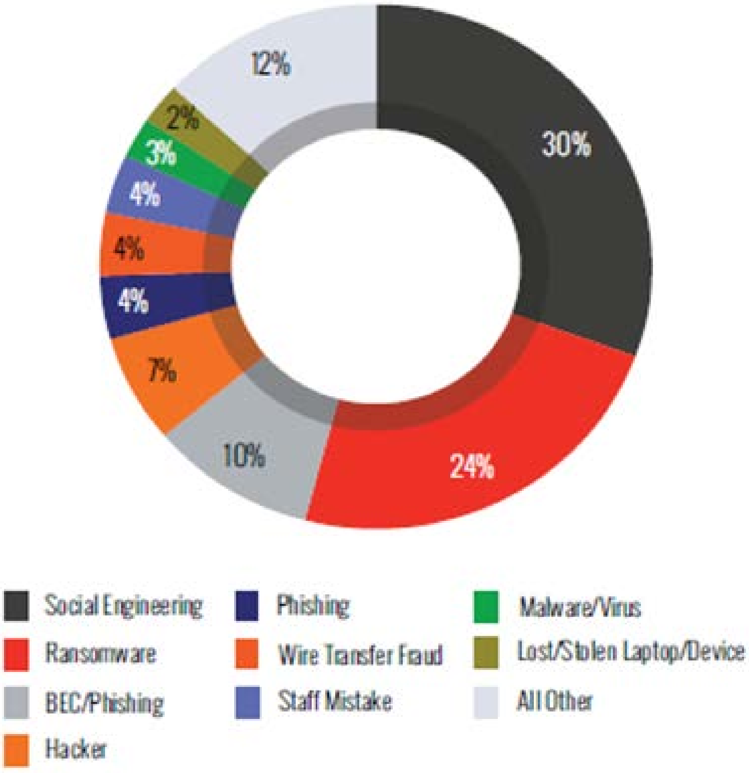


Source: NetDiligence Cyber Claims Study, 2019 Report

Percentage of Claims by Cause of Loss SMEs



Percentage of Claims by Cause of Loss
SMEs - 2014-2018
(N=2,003)



Percentage of Claims by Cause of Loss
SMEs - 2018
(N=640)

Source: NetDiligence Cyber Claims Study, 2019 Report

Insurance Will Cover It

- Depends on your policy.

- Most policies do not cover social engineering or cyber 'fraud,' so read your fine print.

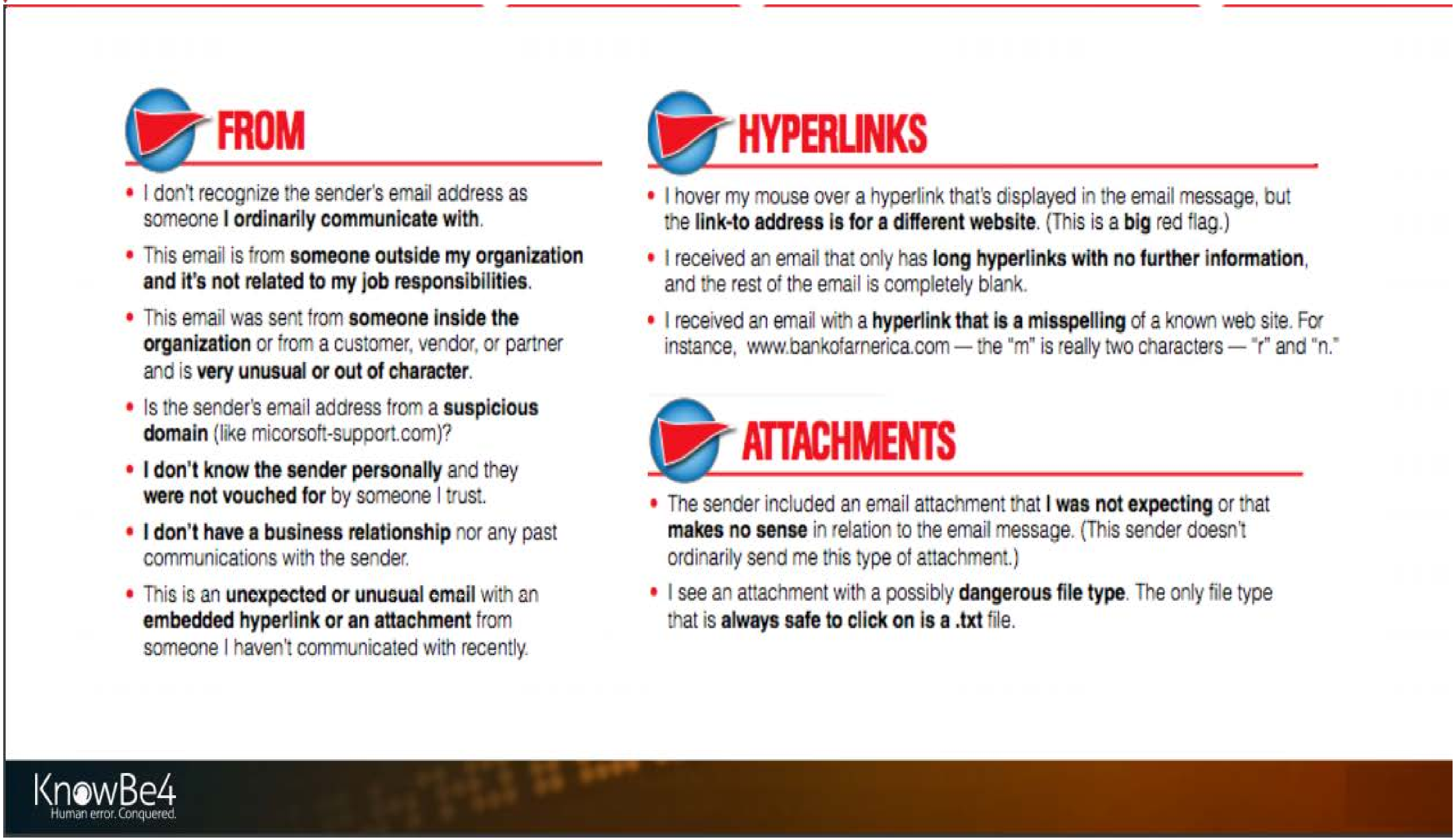
How to Respond?

If you think you have been breached …

- Initiate your incident response plan!
- Or if no plan (invest in a plan!):
  - Stop all wire transfers immediately and contact your bank
  - Unplug and remove from your network any suspected compromised device
  - Scan your network, endpoints and servers looking for “indicators of compromise” and “vulnerabilities” that may have been exploited
  - Engage a cyber security firm to do a forensic investigation
  - Depending on that outcome or if money is missing, involve law enforcement, your attorney and your insurance firm
  - Change all of your passwords, ALL of them

See FBI BEC Checklist in download for more detail

Arm Yourself & Employees



FROM

- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address from a **suspicious domain** (like micorsoft-support.com)?
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any past communications with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I haven't communicated with recently.

HYPERLINKS

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link-to address is for a different website**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information**, and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com — the "m" is really two characters — "r" and "n."

ATTACHMENTS

- The sender included an email attachment that **I was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me this type of attachment.)
- I see an attachment with a possibly **dangerous file type**. The only file type that is **always safe to click on is a .txt** file.

KnowBe4
Human error. Conquered.

Prevention Before the Breach - Administrative

Policy & Procedure

- Institute policies and procedures to protect the company
- Ask your finance team to verify vendor payment requests via phone (on a validated number)
- Ask your HR team to verify changes in employee withholding

  or direct deposit via phone (on a validated number)
- Tighten your (international) wire transfer policies, and include

  a wire transfer time delay
- For large amounts require validation from the CFO/CEO verbal and written

Prevention Before the Breach - Administrative

Training – Security Awareness, Phishing & Information Handling

- Implement security awareness training for all employees
- Implement role specific training for those handling confidential information
- Security awareness trainings and phishing campaigns

Prevention Before the Breach – Technical

Access Control

- Enable two-factor authentication for all account logins
- Confirm two-factor is implemented for all users on Office 365
- Enforce strong password policies. Educate employees on reusing passwords and the risks associated.

Prevention Before the Breach – Technical

Secure Email

- Create visual indicators so emails from external addresses will be obvious to your staff
- Block auto-forwarding email capabilities to make it hard for attackers to hide
- Require encrypted/secure email for all sensitive operations/actions
- Implement server side changes to require validation of the sender's domain (DMARC/SPF)
- Routinely audit email rules for all users looking for odd rules or unusual file locations

Questions?

Doug Davidson
Director of Information Technology Services
GBQ
614-402-5588
ddavidson@gbq.com

Lacy Rex
VP, Cyber Strategic Leader
Oswald Companies
513-716-6002
lrex@oswaldcompanies.com

DIY Security: Self-Assess Your Email Security v. Business Email Compromise
Recorded webinar plus tools to use
https://gbq.com/security-self-access-covid-19-remote-infrastructure-webinar/

KnowBe4 Free Phishing Security Test
What percentage of your employees are Phish-prone?
https://info.knowbe4.com/phishing-security-test-partner?partnerid=001a000001kmOjjAAE

Free KnowBe4 Kevin Mitnick Home Internet Security course free to us to help us protect you.
https://www.knowbe4.com/homecourse
(Don't like to click on redirected URLs? Cut & paste this link into your browser)
password: homecourse

Business Email Compromise Checklist

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Review the checklist below for immediate actions:

IMMEDIATE ACTIONS

Internal Actions

□ Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) – looking for unusual activity

□ Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?

□ Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as "auto forward" or "auto delete"

□ Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage

□ Review all requests that asked for a change in payment type or location. ***Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend.*** **

Reporting the Incident

□ Contact your bank

- □ Determine the appropriate contact at your bank, who has the authority to recall a wire transfer
- □ Notify your bank you have been the victim of a Business Email Compromise

  - AND -

- □ Request a wire recall or SWIFT Recall Message

  - AND -

- □ Request they fully cooperate with law enforcement

□ Report the incident (or attempt) to the FBI at www.IC3.gov

- □ Provide all details for the beneficiary: account numbers, contact information, names

□ Contact your local FBI Field Office

PREVENTION & RECOGNITION

□ Does the Routing Number provided to you, resolve to the expected bank used by the other party? *(Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S?)*

Possible websites to verify a Routing Number:

a. The Federal Reserve www.FRBServices.org
b. American Bankers Association https://routingnumber.aba.com

□ Call a known/trusted phone number or meet in person to confirm the wire transfer information provided to you, matches the other party's information

□ Hover you cursor over suspicious email addresses – Looking for indications of Display Name Deception or Spoofing

□ DO NOT hover on ***links*** within emails, as simply hovering *may* execute commands.

□ Regularly check your email account log-in activity for possible signs of email compromise

□ Regularly check your email account for new "rules", such as email forwarding and/or auto delete

□ Be cautious of "new" customers, suppliers, clients and/or others you don't know who ask you to:

a. …open or download any documents they send

- OR -

b. …sign into a separate window or click on a link to view an invoice or document

- OR -

c. …provide sensitive Personal or Corporate information

□ Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.

a. Where did you get the account data?
b. Is this the correct account number?