



Reducing Your Risk of Business Email Compromise by 90%

Agenda



- Jeremiah School Background
- Innova Overview
- Business Email Compromise
 - Types of Attacks & Scams
 - Real-world Examples
 - How to Reduce Your Risk
 - What To Do When Compromised
- Q&A



Jeremiah School

CEO, Innova Technologies

- 17 years of IT experience
- 3+ years of focused Cybersecurity experience
- 12+ years leading Innova
- Provides vCIO and vCISO services to Accounting Firms, Law Firms, Manufacturing & Distribution, Engineering, Construction, Electric Contractors, and Executives.

Innova Capabilities



Do it for you or with you

Managed Security Services

- Cybersecurity Assessments
- Security Awareness Testing & Training
- Best Practices Framework Alignment
- Patch Management
- Endpoint Detection
- Email System Hardening
- Two Factor Authentication
- Password Management
- IT Policy Review and Development
- Security Information and Event Mgmt.

Managed IT Services

- 24/7 Quick Response Help Desk
- 24/7 Device Monitoring & Alerting
- Backup & Disaster Recovery
- Network Infrastructure
- Solution Engineering
- Best Practice Framework Alignment
- Move, Add, Changes
- Asset and Lifecycle Management

BEC Overview

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

2019 FBI Internet Crime Complaint Center Report

By Victim Count

Crime Type	Victims
Phishing/Vishing/Smishing/Pharming	114,702
Non-Payment/Non-Delivery	61,832
Extortion	43,101
Personal Data Breach	38,218
Spoofing	25,789
BEC/EAC	23,775
Confidence Fraud/Romance	19,473
Identity Theft	16,053
Harassment/Threats of Violence	15,502
Overpayment	15,395
Advanced Fee	14,607

By Victim Loss

Crime Type	Loss
BEC/EAC	\$1,776,549,688
Confidence Fraud/Romance	\$475,014,032
Spoofing	\$300,478,433
Investment	\$222,186,195
Real Estate/Rental	\$221,365,911
Non-Payment/Non-Delivery	\$196,563,497
Identity Theft	\$160,305,789
Government Impersonation	\$124,292,606
Personal Data Breach	\$120,102,501

Spoofing

- Internal Spoofing
- External & Vendor Spoofing



Account Take Over

- Internal and External Targets
- Liability Issues
- Personal Email Too



Types of Scams

- False Invoice
- CEO Fraud
- Attorney Impersonation
- Voicemail
- HR W2
- Delivery Attempt
- Social Media Alert
- Documents from Scanner
- HR Action Required
- Undeliverable Mail
- MS Teams – User Sent You A Message
- Cloud Storage Out of Space

Peebles Media Group



Loss: \$260,000

Attack Summary

A finance department employee was targeted and tricked by a Whaling attack while leadership officials were on vacation. The spoofed leader asked the employee to simply transfer funds from one account to another. Four payments were made over 8 days, to three different bank accounts.

Post Attack

The attack was uncovered after another employee contacted the Managing Director at their vacation resort to confirm payment transfer. The employee tricked was fired and sued. The bank was able to recover about \$115,000 and Peebles sued the fired employee for the remaining balance of the lost funds. The employee won the court case arguing the company was partly responsible for the scam because it had not provided any training on identifying fraud.

City of Saskatoon



Loss: \$800,000

Attack Summary

City was rehabbing a bridge. The contractor's CFO was impersonated via an email about switching banks. Part of the projects funds were then wired by city employees.

Post Attack

Police and cyber professionals were notified 4 days later. 40K of the funds were recovered within the first few weeks. After a year, a majority of the remaining funds was returned after an investigation which led to the arrest of 2 individuals in Nigera which is rare. It was found that policies at the city were not followed which lead to this theft.

Local Company

Loss: Insurance deductible, digital assets, company downtime



Attack Summary

Company was targeted in BEC attack. Attachment from compromised email lead to the compromise of the users PC. From this PC, commercially available hacking tools were used to gain access into server systems, network components and backups. After manually deleting backups and changing network devices, all PC's and servers were encrypted. A ransom of about \$145k in bitcoin was then demanded.

Post Attack











All production data and backups were lost. Experts were contacted including the FBI, IT, cybersecurity and insurance firms. Log files were gathered and systems rebuilt within 48 hours. It took about 2 more weeks to get all critical systems back online. It's estimated that half of the companies users files were lost. The companies cybersecurity posture drastically changed that day. They continue their cyber journey to this day.

Top 5 Ways to Reduce Business Email Compromise

1. Awareness Testing & Training
2. Payment Verification
3. Confirmation of Requests
4. Multi-Factor Authentication
5. Email System Rules

15 Ways to Protect Your Business from a Cyber Attack

15 Ways To Protect Your Business From A Cyber Attack!

 Security Assessment It's important to establish a baseline and close existing vulnerabilities. When was your last assessment? Date: _____	 Spam Email Secure your email. Most attacks originate in your email. We'll help you choose a service designed to reduce spam and your exposure to attacks on your staff via email.	 Logins ***** Passwords Apply security policies on your network. Examples: Deny or limit User file storage access, enable enhanced password policies, set user screen timeouts, and limit user access.
 Security Awareness Train your users - often! Teach them about data security, email attacks, and your policies and procedures. We offer a web-based training solution and "done for you" security policies.	Did you know? 1 in 5 Small businesses will suffer a cyber breach this year. 81% Of all breaches happen to small and medium sized businesses. 97% Of breaches could have been prevented with today's technology.	 Advanced Endpoint Detection & Response Protect your computers data from malware, viruses, and cyber attacks with advanced endpoint security. Today's latest technology (which replaces your outdated anti-virus solution) protects against file-less and script-based threats and can even rollback a ransomware attack.
 Multi-Factor Authentication Utilize Multi-factor Authentication whenever you can including on your network, banking websites, and even social media. It adds an additional layer of protection to ensure that even if your password does get stolen, your data stays protected.	 Computer Updates Keep Microsoft, Adobe, and Java products updated for better security. We provide a "critical update" service via automation to protect your computers from the latest known attacks.	 Dark Web Research Knowing in real-time what passwords and accounts have been posted on the Dark Web will allow you to be proactive in preventing a data breach. We scan the Dark Web and take action to protect your business from stolen credentials that have been posted for sale.
 SIEM/Log Management (Security Incident & Event Management) Use big data engines to review all event and security logs from all covered devices to protect against advanced threats and to meet compliance requirements.	 Web Gateway Security Internet security is a race against time. Cloud based security detects web and email threats as they emerge on the internet, and blocks them on your network within seconds - before they reach the user.	 Mobile Device Security Today's cyber criminals attempt to steal data or access your network by way of your employees' phones and tablets. They're counting on you to neglect this piece of the puzzle. Mobile device security closes this gap.
 Firewall Turn on Intrusion Detection and Intrusion Prevention features. Send the log files to a managed SIEM. And if your IT team doesn't know what these things are, call us today!	 Encryption Whenever possible, the goal is to encrypt files at rest, in motion (think email) and especially on mobile devices.	 Backup Backup local, backup to the cloud. Have an offsite backup for each month of the year. Test your backups often. And if you aren't convinced your backups are working properly, call us ASAP!
 Cyber Insurance If all else fails, protect your income and business with cyber damage and recovery insurance policies.		

Continuum Managed Services | 295 High Street, 2nd Floor, Boston, MA 02101 | 866.225.7394 | © 2016 All Rights Reserved

Cybersecurity Frameworks



NIST Cybersecurity Framework

Cyber Defense Matrix

	Identify	Protect	Detect	Respond	Recover
Devices					
Applications					
Networks					
Data					
Users					
Degree of Dependency	<div><div>Technology</div><div>Process</div><div>People</div></div>				

What to do When Compromised

Respond

1. Contact Financial Institution Involved
2. Contact IT, Cyber and Insurance Experts
3. Contact the FBI
4. Contact Impacted Clients and Vendors

Questions?

Thank you!

Jeremiah School

920-321-3622

jschool@weareinnova.com