CHELSEA
TECHNOLOGIES

ASA/AFRA 2017 CONFERENCE

BUSINESS EMAIL COMPROMISE

ASA RESTON, VA

parts · distribution · disassembly · recycling

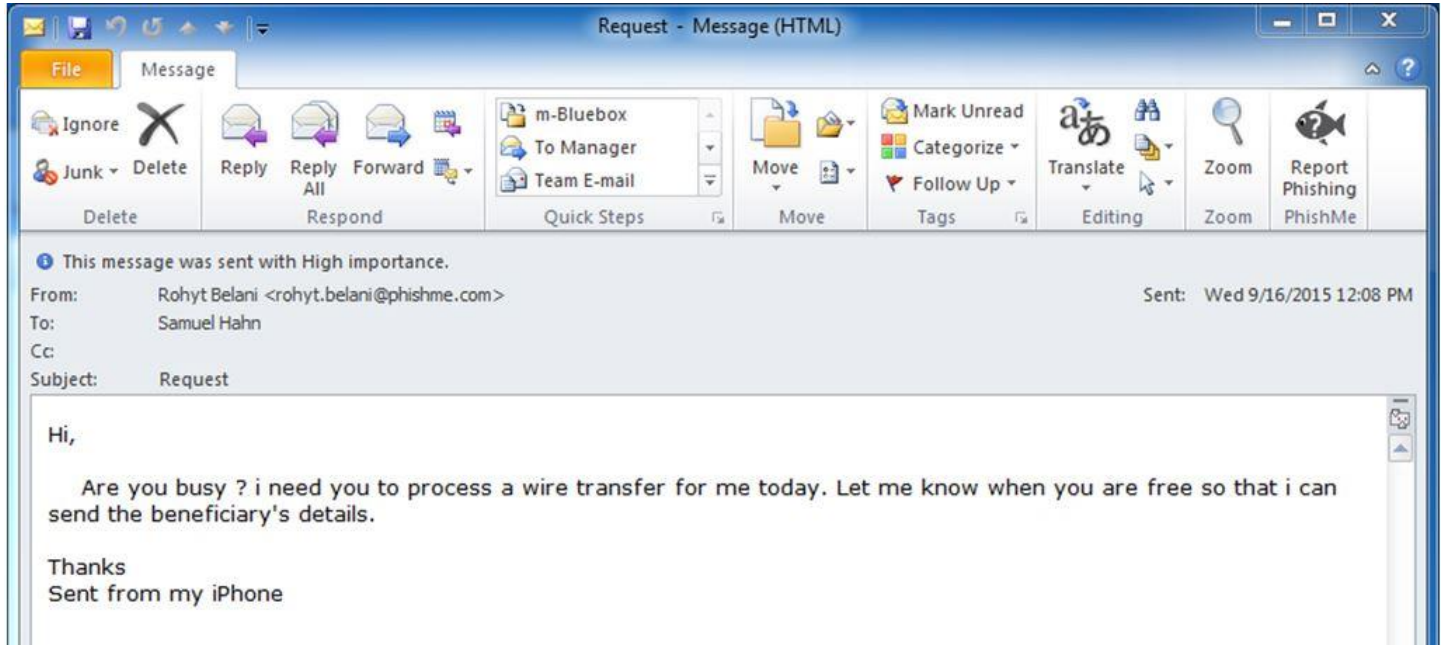
AFRA 9-11 JULY 2017

JULY 2017

Meyer Ben-Reuven – meyer@chelsea-tech.com

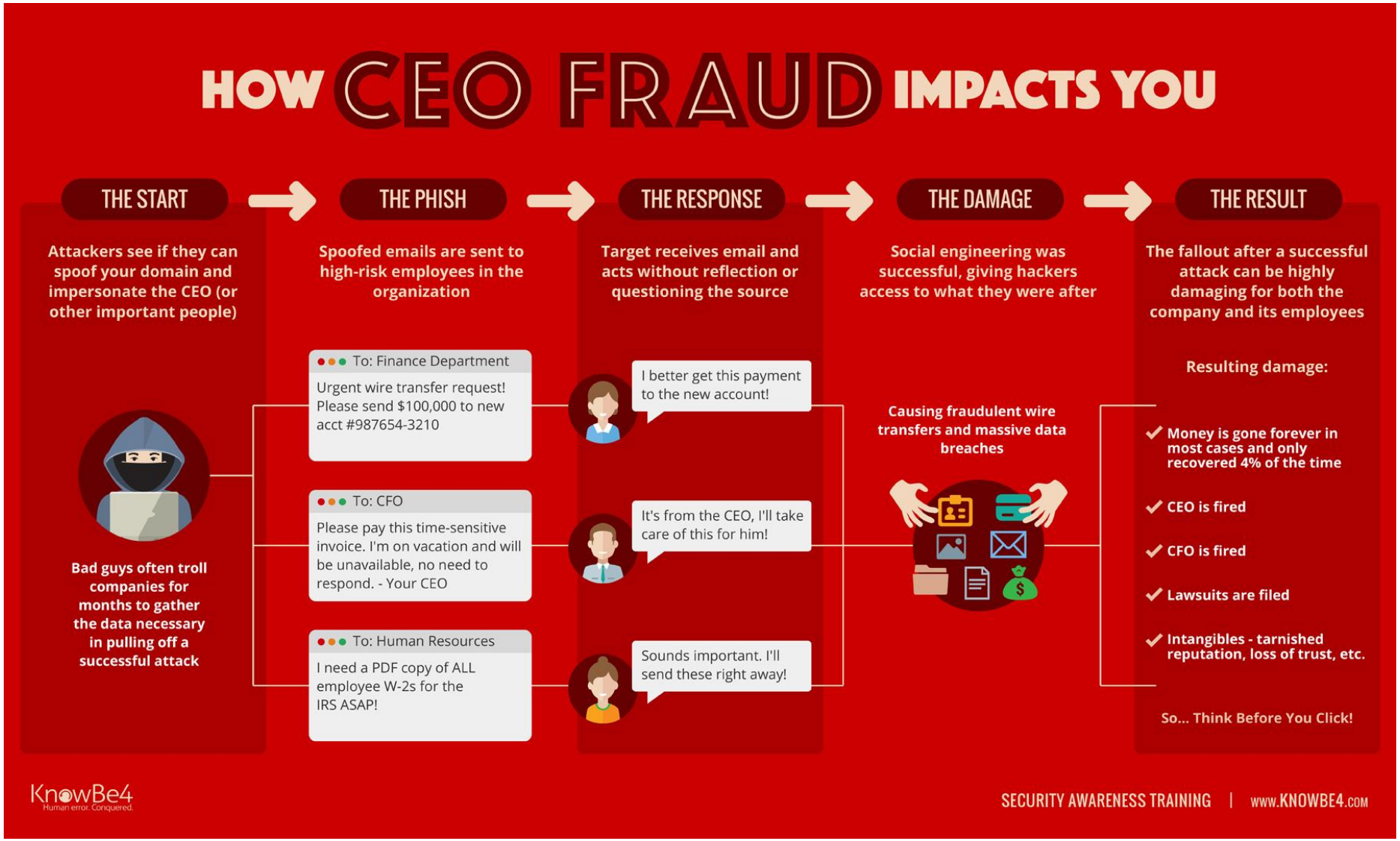
CEO/CFO EMAIL SCAMS

FBI: $2.3 Billion Lost to CEO Email Scams



A typical CEO fraud attack email

CEO/CFO EMAIL SCAMS



ANALYSIS & REMEDIATION

Process to mitigate

- Scan the internal network for malware/viruses
- Inventory of all external systems
- Change passwords everywhere
- Setup Multi-form authentication in external/cloud systems
- Analyze the suspicious emails
- Trace origin of the emails
- Patch all systems with the latest updates from Microsoft
- Ensure all layers for protection are present

- Education of users is priority
- Ensure backups are running (outside the offices)
- If Fraud has been committed and money has been lost, report to FBI
- Unfortunately FBI will not deal with anything less than $3 Million Dollars
- If money has been transferred, you can still recoup some of it if done within 72 hours (you must be very lucky)

CYBERSECURITY GRADING SYSTEM

CLIENT NAME	.	+	% Fulfilled	% Missing	-	DATE	7/11/2017
			84%	16%			

GENERAL & REPORTING

		AREA	DESCRIPTION	V.
1	☐	Company CISO	Chief Information Security Officer	
2	☐	vCISO	CT-CybSec - Virtual CISO	
3	☐	Penetration Testing	CT-CybSec - Third Party	
4	☑	Cyber Insurance	Chubbs - recommended	
5	☐	Production Site (Colocation)	Tototwa NJ	
6	☑	DR Site (Colocation)	NAP Miami	
7	☐	Quarterly DDQ	CT-CybSec - Report	
8	☑	DR Plan	CT-CybSec - Report	
9	☑	BCP Plan	CT-CybSec - Report	
10	☑	Infosec Manuals	CT-CybSec - Report	
11	☑	Reporting	CT-CybSec - Report	
12	☑	Incident Response	CT-CybSec	
13	☐	Vendor DDQ	CT-CybSec	
14	☑	SPF / DKIM Records	CT-CybSec	
15	☑	Email Encryption	CT-CybSec	
16	☑	Managed Security Services	CT-CybSec	
17	☐	Tabletop Exercise	CT-CybSec	
18	☐	Member of ISAC	CT-CybSec	
19	☐	Local Agencies Contact	CT-CybSec	
20	☐	Audited by Regulator+Score	CT-CybSec	
21	☐	Azure Cold DR Site	CT-CybSec	
22	☐			

SOFTWARE

		AREA	DESCRIPTION	V.
1	☑	Email Protection	Mimecast	
2	☑	Multi-Factor Authentication	DUO Security	
3	☑	Anti-Virus	Trend-Micro Anti-Ransomware	
4	☑	Anti-Malware	Malwarebytes - Anti-Ransomware	
5	☑	Malware Sleeper/Fileless Attacks	Minerva Labs - Anti-Ransomware	
6	☑	DNS Protector	Cisco Umbrella - OPENDNS	
7	☑	Mobile Device Management	Continuum/IBM MaaS360	
8	☑	Data Loss Prevention	CT-CybSec	
9	☑	Education	KnowBe4	
10	☑	CyberThreat Monitor Production	NetWatcher Production	
11	☑	CyberThreat Monitor DR Site	NetWatcher DR Site	
12	☑	Onsite Backups	QNAP NAS Device	
13	☑	Online Backups	CT-Vault IASO	
14	☐	IoT - Internet of Things	CT-CybSec - IoT	
15	☑	Patch Management	CT-CybSec - Continuum	
16	☑	Vulnerability Scanning	CT-CybSec - NetWatcher	
17	☑	Mobile Device Encryption	CT-CybSec - Bitlocker	
18	☑	System/Network Inventory	CT-CybSec - Auvik	
19	☐	Secure Internet File Sharing	CT-CybSec - Egnyte	
20	☐	Cyber attack simulator	CT-CybSec - Cymulate	
21	☐	End Point Protection	CT-CybSec - MS Lapse	
22	☐	Cloud Security	CT-CybSec - Avanan	

PROGRAMMING

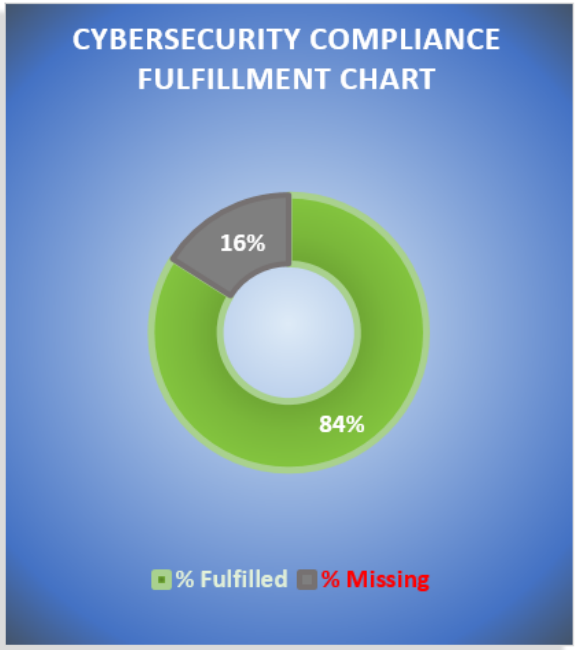
		AREA	DESCRIPTION	V.
1	☑	Local Admin Rights	CT-CybSec - GPO Policy	
2	☑	Lockdown Appdata Folder	CT-CybSec - GPO Policy	
3	☑	Complex Password Policy	CT-CybSec - GPO Policy	
4	☑	USB/Removable Policy	CT-CybSec - GPO Policy	
5	☑	Secured Remote Access	CT-CybSec	
6	☑	Web/Application Filtering	CT-CybSec - Fortigate	
7	☑	WIFI Hardening	CT-CybSec	
8	☑	Compliant Email Disclaimer	CT-CybSec	
9	☐	Vendor Onboarding	CT-CybSec	
10	☐	Data in Rest Encryption	CT-CybSec	
11	☐	State Laws (MS, Privacy Laws)	CT-CybSec	
12	☐	Behavioral Reputation	CT-CybSec	
13	☐			
14	☐			
15	☐			

HARDWARE

		AREA	DESCRIPTION	V.
1	☑	Firewall Production	Next Generation Firewall/UTM	
2	☑	Firewall Production HA	High Availability in DR Site	
3	☑	Firewall DR Site	Next Generation Firewall/UTM	
4	☐	Firewall DR Site HA	High Availability in DR Site	
5	☐	Home Firewalls	Firewalls for home use	
6	☐			
7	☐			
8	☐			
9	☐			
10	☐			
11	☐			
12	☐			
13	☐			
14	☐			
15	☐			

CYBERSECURITY GRADE

B - SECURED



QUESTIONS & ANSWERS

Meyer Ben-Reuven
meyer@chelsea-tech.com
C - 917-251-0970
O-954-454-9797 / O-212-966-3355
www.chelsea-tech.com