AMERICAN BANKRUPTCY INSTITUTE

Annual Spring Meeting

CONCURRENT SESSION

The Impact of Business Email Compromise in the Bankruptcy Arena: Strategies and Tools to Protect Bankruptcy Participants

Hosted by the Bankruptcy Litigation, Commercial & Regulatory Law and Financial Advisor and Investment Banking Committees

Hon. Bruce A. Harwood, Moderator
U.S. Bankruptcy Court (D. N.H.); Concord

Phil Denning
ICR Communications; New York

David G. Fine
Federal Bureau of Investigation Cyber Division; Washington, D.C.

William T. Repasky
Frost Brown Todd LLP; Louisville, Ky.

Keith Wojcieszek
Kroll; Washington, D.C.

2024

The Impact of Business Email Compromise in the Bankruptcy Arena: Strategies and Tools to Protect Bankruptcy Participants
ABI Spring Conference**,** Friday, April 19th at 2:15 PM

Panel Agenda

Moderator: Judge Bruce Harwood

Panel: David Fine, SSA with the FBI
Keith Wojcieszek, with Kroll
Bill Repasky, with Frost Brown Todd LLP
Phil Denning, with ICR, LLC

1. **Introductions**

   Judge Harwood welcomes attendees and invites panelists to introduce themselves

   "Let's dive right in. The first question I have is for the FBI - Supervisory Special Agent Fine, can you please tell us what Business Email Compromise is and the size of the problem we have on our hands?

2. **What is Business Email Compromise?**

   a. Define BEC for purposes of today's panel discussion

      i. BEC attacks originating from an email account's take-over versus spoofing

      ii. Internal BEC a/k/a CEO compromise vs. Third-Party BEC

         1. Attacks premised on known vendor relationship

            e.g., You (victim) owe vendor/party money under a contract or settlement, but an email is received from the vendor stating it has changed banks and directing your payment to the new bank account.

         2. Attacks premised on fake vendor relationship

            e.g., Fictious vendor invoice received to Accounts Payable

         3. Attacks targeting "victim's" customers Customer relationship

            a. e.g., Your customers (or others who owe money to you) receive an email telling them your own banking information

has changed and their upcoming payment must be sent to that new bank account.

iii. Its typically about getting money, but not always

1. Stealing employee information, personally identifying information, trade secrets, etc.

iv. Common TA tactics during attacks

1. Imposition of "account forward rules"
2. Urgency
3. Secrecy
4. Unavailability of supposed sender

v. BEC data from IC3 data and Verizon's DBIR Report

1. Overall number of attaks
2. Annual dollar amounts
3. Individual example of large dollar loss events.

vi. Nature of targets

1. High & low sophisticated victims
2. All industries are targets
3. Bankruptcy lawyers, trustees and vendors – Anyone who uses email or SMS text messaging

c. Trends or forecast for future threat vectors of BEC attacks

~ AI generated/enhanced attacks

~ Latest FBI intel on emerging BEC tactic and targets

d. Unique bankruptcy issues

Transparency required for the benefit of all stakeholders in bankruptcy incidentally benefits fraudsters.

e.g., public disclosure of relationships between participants, payment flows between participants, etc.

3. What happens when it happens?

a. First Hour/First Steps:

i. Build a team (Forensic consultant, lawyer, Victim's IT and Victim's business leadership)

ii. Recover fraudulently transferred funds

1. Working with beneficiaries' RDFI's

2. Financial Fraud Kill Chain

~ Domestic vs. International

iii. Notify victim's financial institution(s)

1. ODFI's role in funds recall

2. Prevention of second-level attacks

iv. Consideration for notice to other vendors/customers

v. Notice to insurance provider

vi. Why, when and how to involve law enforcement authorities

~ FBI/Secret Service/Local law enforcement

~ IC3 filing: How and why

b. Second steps/ Hour 2 and beyond:

i. Quantify TA's access and lateral movement

ii. Kick the TA out of any infiltrated email servers

iii. Bankruptcy specific issues

1. Notice and pleading issues

iv. Statutory notifications

v. Data breach notification

a. Assess applicable law as to scope of covered events

b. Planning data breach notification communications

vi. Communications strategy

1. Internal strategy
2. Affected counter-parties
3. Stakeholders
4. Press and public-facing announcements

vii. Build back better

4. Prevention Strategies

i. Technology

ii. Training/education

1. Teach, and re-teach, awareness
2. Teach culture of verification

iii. Processes

1. Technology and training will fail, but procedures typically do not.

iv. Contract terms and conditions

1. Business contracts with customers and vendors
2. Bankruptcy settlement agreement terms

5. The money is gone and everyone is mad at each other - Law in the area of BEC

a. Legal overview of the decisional laws

i. Banks versus victims

ii. UCC Article 4A

1. Victim vs. ODFI
2. Victim vs. RDFI
3. Account agreement and online banking contracts

iii. Victim vs victim; e.g., customer vs. vendor

1. Contracts between the parties

a. Considerations for “new” contract terms in form contracts

b. Settlement Agreement terms

2. Case law precedent

a. Contract performance

i. If a payment is not received by the entitled party, it is a simple payment breach

b. Comparative fault analysis

b. Resolution process options and experiences

i. Contractual forum directives

ii. Extrajudicial processes

1. Formal vs. informal mediation

2. Pros and cons of different options

EN10007.Public-10007 4856-5315-2684v3

Business Email Compromise

What is Business Email Compromise ("BEC")?

A fraudster uses email or SMS text to impersonate one company to convince another company, or alternatively impersonate a senior officer in the company to convince company employee, to send a payment to a bank account controlled by the fraudster.

Common Steps in a BEC Attack

1.(A) Fraudster gains access to a business email account, either by hacking the company's computer servers or by a phishing attack.

1(B) Fraudster "spoofs" an employee's email address, such that it appears to the reader that it is being sent by a known business acquaintance.

2. Fraudster studies email traffic to learn payment patterns, if "inside" the hacked machine.

3. Fraudster either (a) installs "email forwarding rule" to exclude the compromised employee from the email chain, or (b) waits until the executive is unreachable.

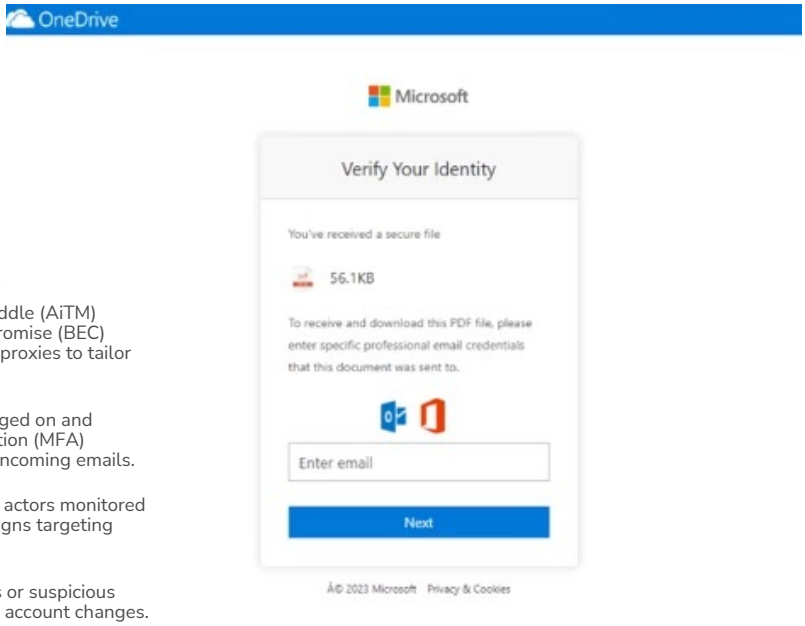
4. Fraudster sends mail, to a person with payment authority, requesting a payment and/or altering existing payment directions (changing banking routing and account number details).

5. Victim directs its bank to send an ACH or wire transfer to a bank account controlled by the fraudster.

6. Once the payment is received, the fraudster drains the bank account and disappears.

Microsoft Observations of AiTM and BEC Campaigns

- Microsoft has reported Adversary-in-the-Middle (AiTM) campaigns leading to Business Email Compromise (BEC) where threat actors have leveraged indirect proxies to tailor phishing pages to targets.
- Following credential stealing, the actors logged on and configured additional multifactor authentication (MFA) methods and inbox rules to move or delete incoming emails.
- Upon gaining access to victim's inboxes, the actors monitored incoming emails and began phishing campaigns targeting other organizations.
- It is recommended to monitor for anomalous or suspicious activity surrounding user account logins and account changes.



KROLL

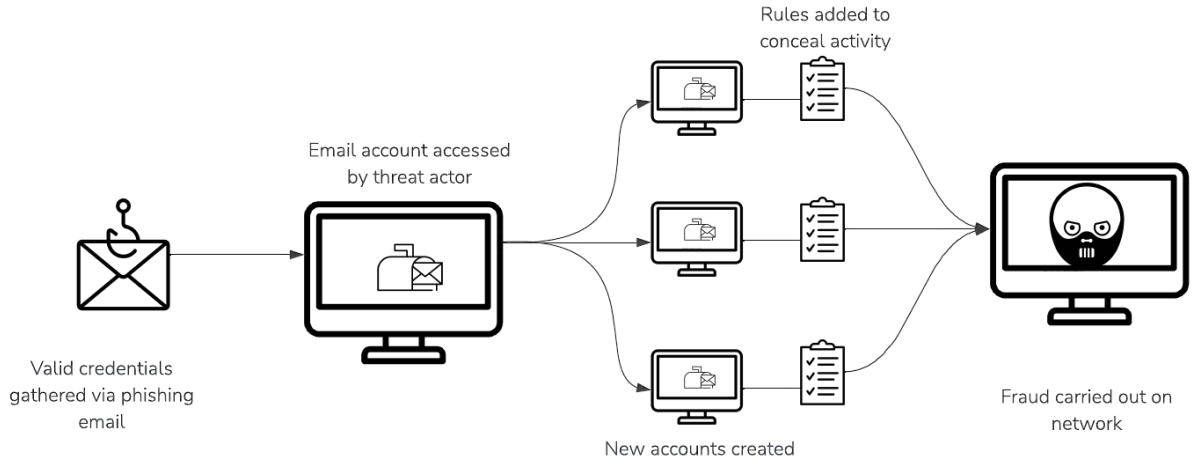
MFA Bypass on the Rise

- Observing an increase in large-scale Adversary-in-the-Middle (AiTM) phishing and BEC attacks
- **90%** had **MFA in place** at the time of unauthorized access.
- Sectors notably targeted:
  - Professional Services
  - Banking
  - Financial industries
- Toolkits used by threat actors:
  - EvilProxy
  - Evilginx2
  - W3LL
- Exploitation activities included:
  - Payroll redirection
  - Invoice payment fraud
  - Data exfiltration
  - Extortion

How a typical AiTM attack plays out

1. AiTM attack typically begins with a phishing email sent to a user
2. Phishing email contains a link to a spoofed domain that is really a credential harvesting website.
3. A proxy tool used by the actor(s) sits in between this spoofed domain credential harvesting website and a legitimate M365 login form.
4. Once the user enters their credentials into the spoofed domain credential harvesting website and satisfies MFA requirements, **the proxy tool steals the legitimate session ID token.**
5. In turn, the actor(s) can reuse this legitimate session ID token and bypass multifactor authentication ("MFA") to the user's account.

Email Compromise Attack Chain



KROLL 7

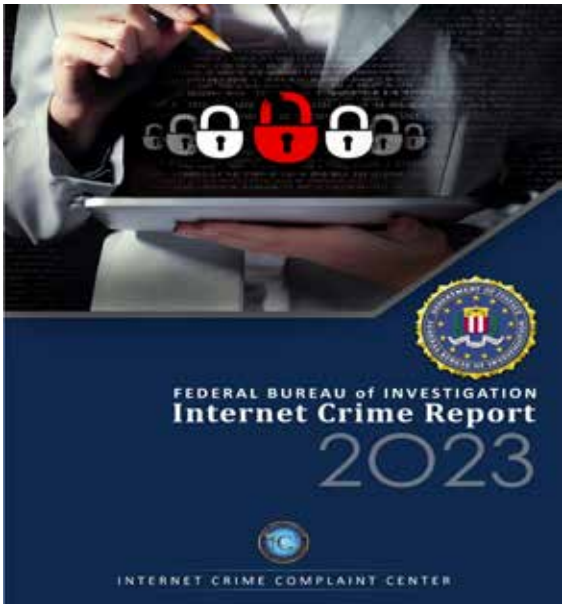
Example: Typical Business Email Compromise

- Financially motivated actors
- Search terms are typically run by the actors to identify pending or open invoices and business contacts, which they then target and orient themselves against.
  - *Examples:*

Row #	Search Term	Date & Time
4	invoice	02/09/2022 14:16:32 UTC
5	ach	02/09/2022 14:08:07 UTC
6	wire	02/09/2022 14:07:43 UTC
8	account	02/08/2022 14:56:16 UTC
9	payment	02/08/2022 13:30:53 UTC
13	transfer	02/05/2022 14:45:20 UTC

8

BEC is a really BIG & EXPENSIVE problem.



2023 CRIME TYPES

By Complaint Count			
Crime Type	*Complaints*	*Crime Type*	*Complaints*
Phishing/Spoofing	298,878	Other	8,808
Personal Data Breach	55,851	Advanced Fee	8,045
Non-payment/Non-Delivery	50,523	Lottery/Sweepstakes/Inheritance	4,168
Extortion	48,223	Overpayment	4,144
Investment	39,570	Data Breach	3,727
Tech Support	37,560	Ransomware	2,825
BEC	21,489	Crimes Against Children	2,361
Identity Theft	19,778	Threats of Violence	1,697
Confidence/Romance	17,823	IPR/Copyright and Counterfeit	1,498
Employment	15,443	SIM Swap	1,075
Government Impersonation	14,190	Malware	659
Credit Card/Check Fraud	13,718	Botnet	540
Harassment/Stalking	9,587		
Real Estate	9,521		
Descriptors*			
Cryptocurrency	43,653	Cryptocurrency Wallet	25,815

*These descriptors relate to the medium or tool used to facilitate the crime and are used by the IC3 for tracking purposes only. They are available as descriptors only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

2023 INTERNET CRIME REPORT 23

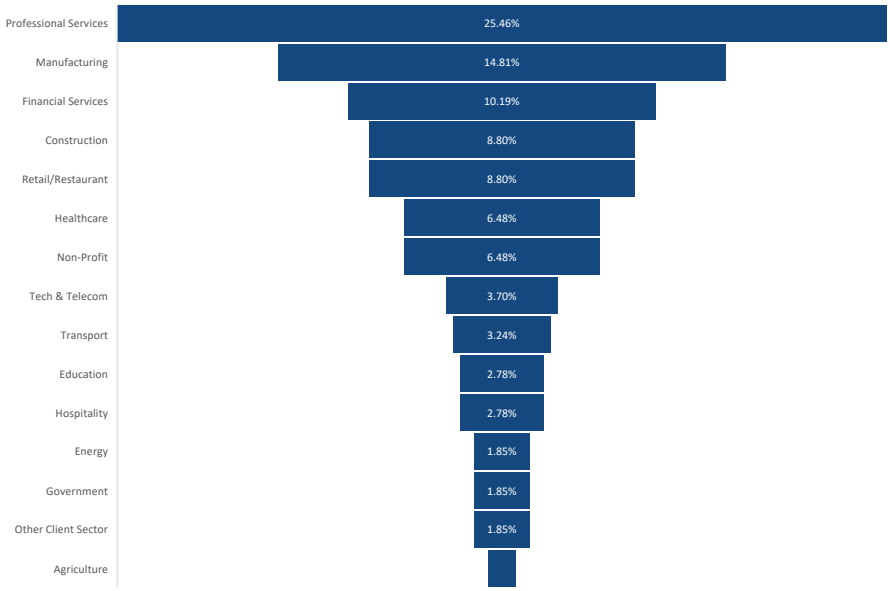
LAST-THREE-YEAR COMPLAINT LOSS COMPARISON

By Complaint Loss			
Crime Type	2023	2022	2021
Advanced Fee	$134,516,577	$104,325,444	$98,694,137
BEC	$2,946,830,270	$2,742,354,049	$2,395,953,296
Botnet	$22,422,708	$17,099,378	N/A
Confidence Fraud/Romance	$652,544,805	$735,882,192	$956,039,739
Credit Card/Check Fraud	$173,627,614	264,148,905	$172,998,385
Crimes Against Children	$2,031,485	$577,464	$198,950
Data Breach	$534,397,222	$459,321,859	$151,568,225
Employment	$70,234,079	$52,204,269	$47,231,023
Extortion	$74,821,835	$54,335,128	$60,577,741
Government Impersonation	$394,050,518	$240,553,091	$142,643,253
Harassment/Stalking	$9,677,332	$5,621,402	N/A
Identity Theft	$126,203,809	189,205,793	$278,267,918
Investment	$4,570,275,683	$3,311,742,206	$1,455,943,193
IPR/Copyright and Counterfeit	$7,555,329	$4,591,177	$16,365,011
Lottery/Sweepstakes/Inheritance	$94,502,836	$83,602,376	$71,289,089
Malware	$1,213,317	$9,326,482	$5,596,889
Non-Payment/Non-Delivery	$309,648,416	$281,770,073	$337,493,071
Other	$240,053,059	$117,686,789	$75,837,524
Overpayment	$27,955,195	$38,335,772	$33,407,671
Personal Data Breach	$744,219,879	$742,438,136	$517,021,289
Phishing/Spoofing	$18,728,550	$160,015,411	$126,383,513
Ransomware	$59,641,384	$34,353,237	$49,207,908
Real Estate	$145,243,348	$396,932,821	$350,328,166
SIM Swap	$48,798,103	$72,652,571	N/A
Tech Support	$924,512,658	$806,551,993	$347,657,432
Threats of Violence	$13,531,178	$4,972,099	N/A

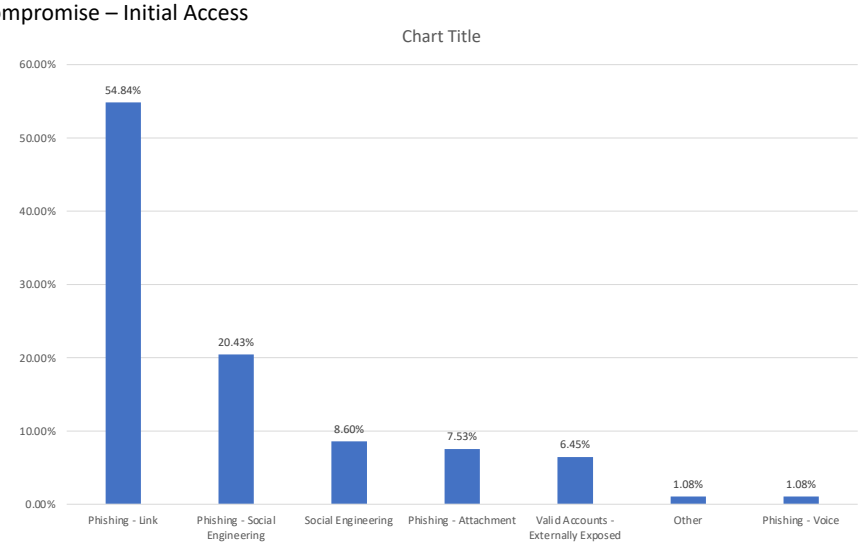
When Your Organization is Attacked

- When in doubt, assume the worst.
  - Out-of-band contact with the “real” counterparty.
- Minutes (literally) matter, as wired or ACH funds are nearly instantly available to the fraudster.
- Invoke your Incident Response Plan immediately.
- Call your banker immediately.
  - Talk in-person to your banker
  - No voicemails & No emails
- Reversing entries/retrieval orders; 314(b) and Reg. P; and Adverse Claim to Deposit Act & Uniform Indemnification Agreements.

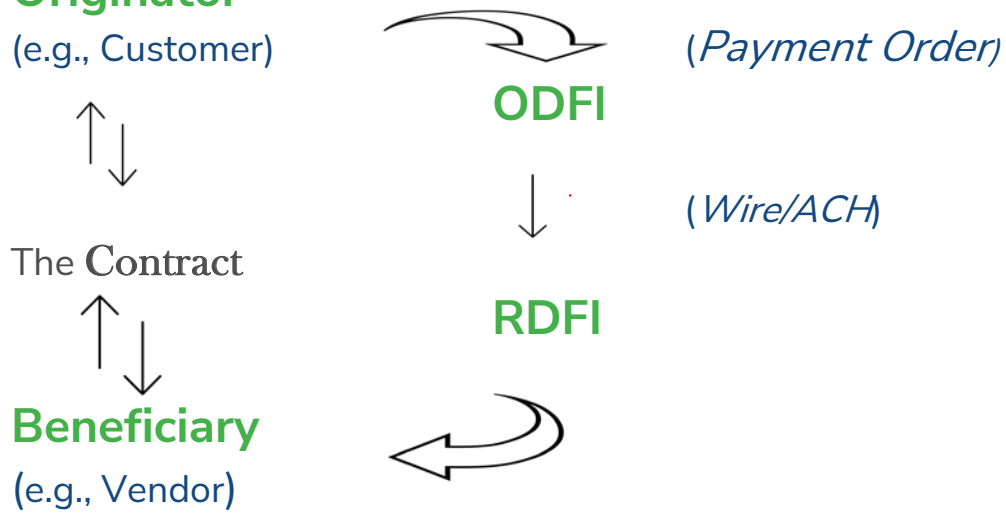
Email Compromise – By Sector – TOP 5



Email Compromise – Initial Access



ePayment Flow Model



ALL "PAYMENT" ATTACKS

Know what laws and which regulations apply

1. **Is Customer a consumer or commercial entity?**
2. **What payment method?**
3. **What instrumentality**
   - Attack on machine vs attack on person
4. **Plan to be instantly brilliant**
   - ODFI – Inform, recover & mitigate steps
   - Law enforcement - FBI's Kill Chain & RAT
   - Organization's "Incident Response Plan"
5. **Lawyer's roles in pre-planning, response and post-operations**

Victim vs. Its Bank

Commercial Account BEC:

UCC's Article 4A governs "payment orders"

Risk of loss allocated based upon **authentication** of Sender

Rule of Thumb #1: Financial Institution is liable for payment order made by an unauthorized user.

~ 4A-204

Rule of Thumb #2: Victim who directed its bank to make the e-payment, even if fooled by a BEC fraudster, typically has no claim against its Bank

~ 4A-202(a)

~ UCC preempts most common law claims

Victim vs. Fraudster's Bank

Common allegation is that the incoming wire's named beneficiary did not match the wire's account # at the receiving bank.

UCC's 4A-207:

~ RDFI's typically have no duty to verify that the account # matches the beneficiary named therein

~ Banks typically rely only on the account #

- Read *Comment 2 to 4A-207*

Contra, Studco Building Systems v. 1st Advantage FCU, 1/12/2023, USDC, ED of Va. (Appeal Pending)

ODFI vs. RDFI

ODFI sends at victim's request a Reversing Wire Instruction:

"[a]fter a payment order has been accepted, cancellation or amendment of the order is not effective, *unless the receiving bank agrees or a funds-transfer system rule allows cancellation or amendment without agreement of the bank*."

~ 4A-211(c)

The Counterparties' Battle Royal

Simple Breach of Contract vs. Comparative Fault Analysis

Contract Analysis:

The Party that was supposed to pay under the contract remains obligated to do so, i.e., must pay the same debt twice.

E. g., Peebles v. Carolina Container, et al.; 9/16/2021, USDC ND of FA; 2021 WL 4224009, at *8

Comparative Fault Type Analysis

- Trending predominant analysis
- **Liability is allocated generally based on the relative faults of the parties.**
  - What contract terms existed
  - What protections were in place
  - Authentication steps taken
  - Nature of the fraudulent communications
  - Other variables
- *E.g., Beau Townsend Ford v. Don Hines Ford*, 759 Fed. Appx 348 (Sixth Circuit reversed/remanded District Court's liability based on a pure contract analysis).

Mitigating BEC Risks

✓ Training
✓Technology
✓Processes
✓Contracts

Self Defense

Best Practices

Enable multi-factor authentication whenever offered

Multi-factor strengthens security by requiring a username and password PLUS a one-time code sent to your phone via SMS or an authentication app.

Avoid password reuse and never share your password

Choose long, easily rememberable passphrases and consider using trusted password management software. Don't use your work email for anything but work.

Install the latest patches on all of your devices

Ensure that devices, including smartphones, have the latest patches installed if you are responsible for installing them. This is a first aid kit for vulnerabilities.

Best Practices

Exercise extreme caution with suspicious emails

Be very wary of suspicious emails and phone calls, especially where you are asked to visit a website, open an attachment or provide credentials.

Safeguard your home network

Set complex Wi-Fi passwords and change default administrator credentials on devices like home routers.

Best Practices

Avoid installing unnecessary applications

Installing unnecessary software on laptops and smartphones create new vulnerabilities for your devices, home network, and corporate network. Understand what you are installing and use legitimate App Stores.

Be mindful of the sensitivity or classification of your conversations

When using collaboration tools (e.g. WhatsApp, LINEapp, etc.) be aware of what you share as attackers may use it to target you, your business and those that you know.

Finish your day by logging off and securing paperwork

Physical security is just as important—log off of devices after use. Store sensitive paperwork out of sight and shred it if no longer needed.

Faculty

Phil Denning is a partner at ICR Communications, LLC in New York and heads ICR's special situations group, advising boards of directors and executive leadership of public and private corporations and private-equity firms on a range of issues, from bankruptcies and restructurings, litigation matters, mergers and acquisitions, spin-offs, IPOs, activist campaigns, proxy contests, short-seller attacks, executive transitions and other corporate events that may generate sudden and significant confusion or uncertainty that requires an experienced and specialized communications team to manage. He has expertise advising companies involved in out-of-court and in-court restructurings across a wide range of industries. He also has advised on more than 100 mergers and acquisitions, including friendly, hostile, distressed and go-private transactions. Mr. Denning joined ICR from RLM Finsbury, where he was a principal and member of its U.S. Executive Committee. Prior to that, he was with Marsh & McLennan, head of investor relations at Kroll Inc., and managing director at IR boutique Kehoe, White, Savage & Co. Mr. Denning received his B.S. in finance from Fordham University and his M.B.A. from Fordham's Gabelli School of Business, and he has served as an adjunct professor of business communications and crisis communications at Fordham's undergraduate and graduate business schools.

David G. Fine is with the Federal Bureau of Investigation's Cyber Division in Washington, D.C.

Hon. Bruce A. Harwood is Chief U.S. Bankruptcy Judge for the District of New Hampshire in Concord, appointed to the bench in March 2013. He also serves on the First Circuit's Bankruptcy Appellate Panel. Prior to his appointment to the bench, Judge Harwood chaired the Bankruptcy, Insolvency and Creditors' Rights Group at Sheehan Phinney Bass + Green in Manchester, N.H., representing business debtors, asset-purchasers, secured and unsecured creditors, creditors' committees, trustees in bankruptcy, and insurance and banking regulators in connection with the rehabilitation and liquidation of insolvent insurers and trust companies. He was a chapter 7 panel trustee in the District of New Hampshire and mediated insolvency-related disputes. Judge Harwood is ABI's Vice President-Communication, Information & Technology, and serves on its Executive Committee. He previously served as ABI's Secretary, as co-chair of ABI's Commercial Fraud Committee, as program co-chair and judicial chair of ABI's Northeast Bankruptcy Conference, and as Northeast Regional Chair of the ABI Endowment Fund's Development Committee. He also served on ABI's Civility Task Force. Judge Harwood is a Fellow in the American College of Bankruptcy and was consistently recognized in the bankruptcy law section of *The Best Lawyers in America*, in *New England SuperLawyers* and by *Chambers USA*. He received his B.A. from Northwestern University and his J.D. from Washington University School of Law.

William T. Repasky is a partner with Frost Brown Todd LLP's Louisville, Ky., office and is a former chair of the firm's Financial Services Litigation Practice sub-group. Prior to joining the firm, he was in-house counsel for National City Bank, where his responsibilities included litigation, deposit operations and treasury management (payments) services. Mr. Repasky is experienced with guiding clients in all aspects of financial fraud (traditional and cyber), e-payments and business email compromise (BEC). He regularly counsels on BEC mitigation strategies, fund recovery actions and in handling

BEC disputes, both in litigation and extrajudicially. Mr. Repasky is a frequent author and speaker on BEC attacks, cyberfraud and electronic payments. He received his B.A. from the University of Michigan and his J.D. from Vanderbilt University Law School.

Keith Wojcieszek is global head of Threat Intelligence in Kroll, LLC's Cyber Risk practice in Washington, D.C. He joined Kroll from the U.S. Secret Service, where he served with distinction for 15 years. Mr. Wojcieszek founded and leads Kroll's Cyber Threat Intelligence program, manages a wide range of cybercrime, data-loss and incident-response investigations, and is a trusted advisor to clients involved in compliance-related or sensitive local and global cybersecurity matters. He also has experience working with international stakeholders on complex transnational investigations and initiatives. From 2012-2016, Mr. Wojcieszek was an integral member of protection details for the president, vice president, Homeland Security Advisor to Terrorism and Presidential Chief of Staff. Earlier, from 2012-15, he was with the Counter Assault Team in the Special Operations Division, which often involved coordinating security in varying international environments for the USSS protective mission and incorporated multiple U.S. federal agencies, local law enforcement and foreign government personnel. Earlier in his career, Mr. Wojcieszek led several domestic and global investigations working with the U.S. Department of Justice Computer Crime and Intellectual Property Section (CCIPS) and Office of International Affairs (OIA). From 2004-10, he managed the Electronic Crimes Task Force in support of all electronic crime investigations, computer forensic examinations and cell phone data extraction in the Louisville Field Office District. In this role, he also established the operation of a forensic laboratory, provided expert testimony in multiple state and federal cases, and coordinated training for USSS agents, local law enforcement and industry representatives. A noted authority on cyber and intelligence-related topics, Mr. Wojcieszek has served as a certified expert witness in court proceedings and is frequently asked to speak at public and private conferences, webinars and panel discussions. He received his B.S. in criminal justice from the State university of New York at Buffalo, and his Cyber Security Certificate from Rutgers University.