

CYBERSECURITY:

RISKS & OPPORTUNITIES FOR ASSOCIATIONS



NARdotRealtor



nar.realtor

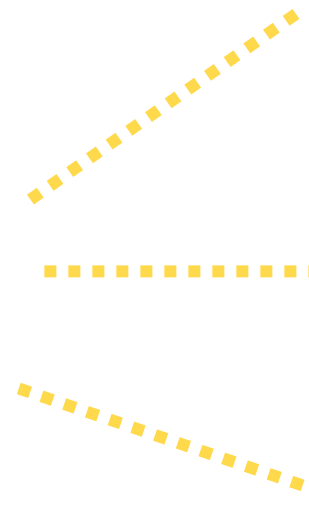




TOPICS

- Coverage & claims
- Phishing
- Claims trends nationwide
- Incident response
- Q & A

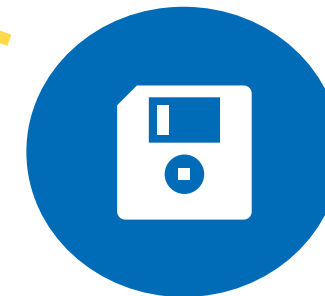
WHY ARE WE HERE?



Loss of Funds



Ransomware



Other Breach
or Loss of Data

CLAIMS HISTORY

- Ransomware
- Network intrusion
- Theft of personal information
- Stolen credit card details
- Malware
- Fraudulent invoices/wire transfers

ARE WE COVERED?

NAR Institutes, Societies & Councils

- State and Local Chapters
- Subsidiaries

State and Local REALTOR® Associations

- Charitable Foundations
- Political Committees
- Educational Endeavors

MLSs wholly-owned and operated by two or more Associations

ARE WE COVERED?

Directors & Officers

Committee Members

Employees

*While acting within
the scope of their
duties on behalf of
the insured entity.*

ARE WE COVERED?

1. **Cyber Liability:** Loss and claims expenses for a Cyber Incident

- Network security failure (i.e. hacking)
 - Failure to properly manage, store, protect or destroy Personal Information
 - Unintentional violation of any privacy or cyber laws
 - Suspected network extortion threat
-
- Payment Card Loss
 - Regulatory Fines & Proceedings

\$1 million claim limit; \$100,000 sublimit on PCL and regulatory fines/proceedings. Deductibles apply.

ARE WE COVERED?

2. Cyber Response

- Cyber Incident Response Expenses
- Digital Data Recovery Costs
- Extortion Expenses

\$1 million claim limit; sub-limit of \$100,000 each claim for response expenses. Deductibles apply.

ARE WE COVERED?

BUT ...

Fraudulent invoices, resulting in the loss of funds are **social engineering** and not covered by the cyber clauses.

REPORTING A CYBER CLAIM



CALL THE CYBER HOTLINE

800-817-2665

Available 24/7

Follow up with an email to
Justin.rose@chubb.com



SEBASTIAN DRYWA

NAR IT Security

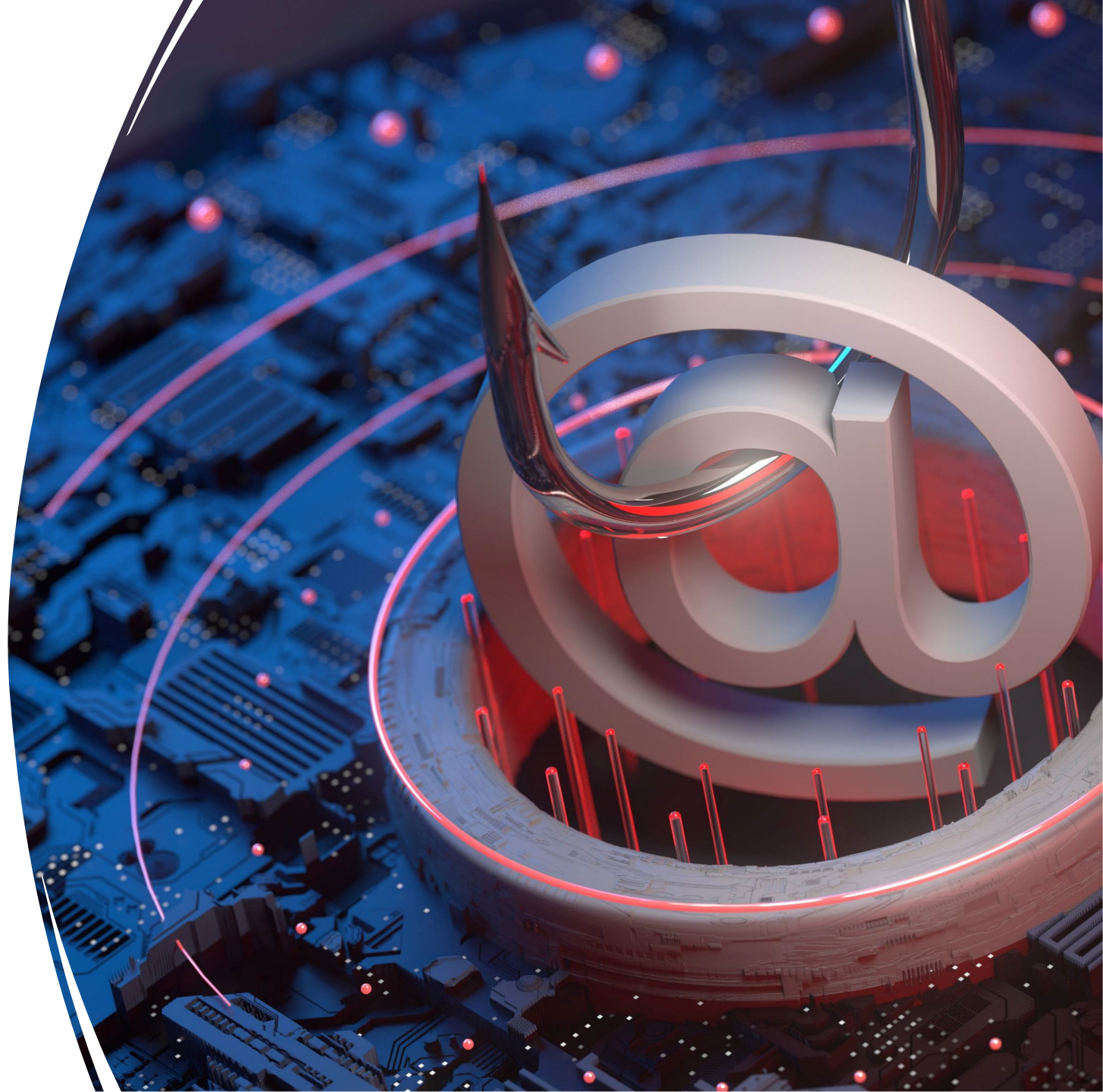


Phishing

Sebastian Drywa
IT Security Director

Phishing. Don't Fall for the Hook.

-
- Email
 - Phone
 - Text messages



Common Features of Phishing Emails

- Too Good To Be True
- Sense of Urgency
- Hyperlinks
- Attachments
- Unusual Sender

It's urgent

The message pressures you to act now — or something bad will happen.

PHISHING WORKS

You get an email or text

It seems to be from someone you know, and it asks you to click a link, or give your password, business bank account, or other sensitive information.

It looks real

It's easy to spoof logos and make up fake email addresses. Scammers use familiar company names or pretend to be someone you know.

What if you fall for a Phishing Scheme

- Alert the others
- Limit the damage
- Follow your company procedures
- Notify customers
- Report it

Limit the damage

Immediately change any compromised passwords and disconnect from the network any computer or device that's infected with malware.

Follow your company's procedures

These may include notifying specific people in your organization or contractors that help you with IT.

Alert others

Talk to your colleagues and share your experience. Phishing attacks often happen to more than one person in a company.

Prevent Phishing Attacks

- Awareness training
- Deploy a safety net and Spam filtering
- Backup your data
- Keep your security up to date
- Develop incident response



Deploy a safety net

Use email authentication technology to help prevent phishing emails from reaching your company's inboxes in the first place.



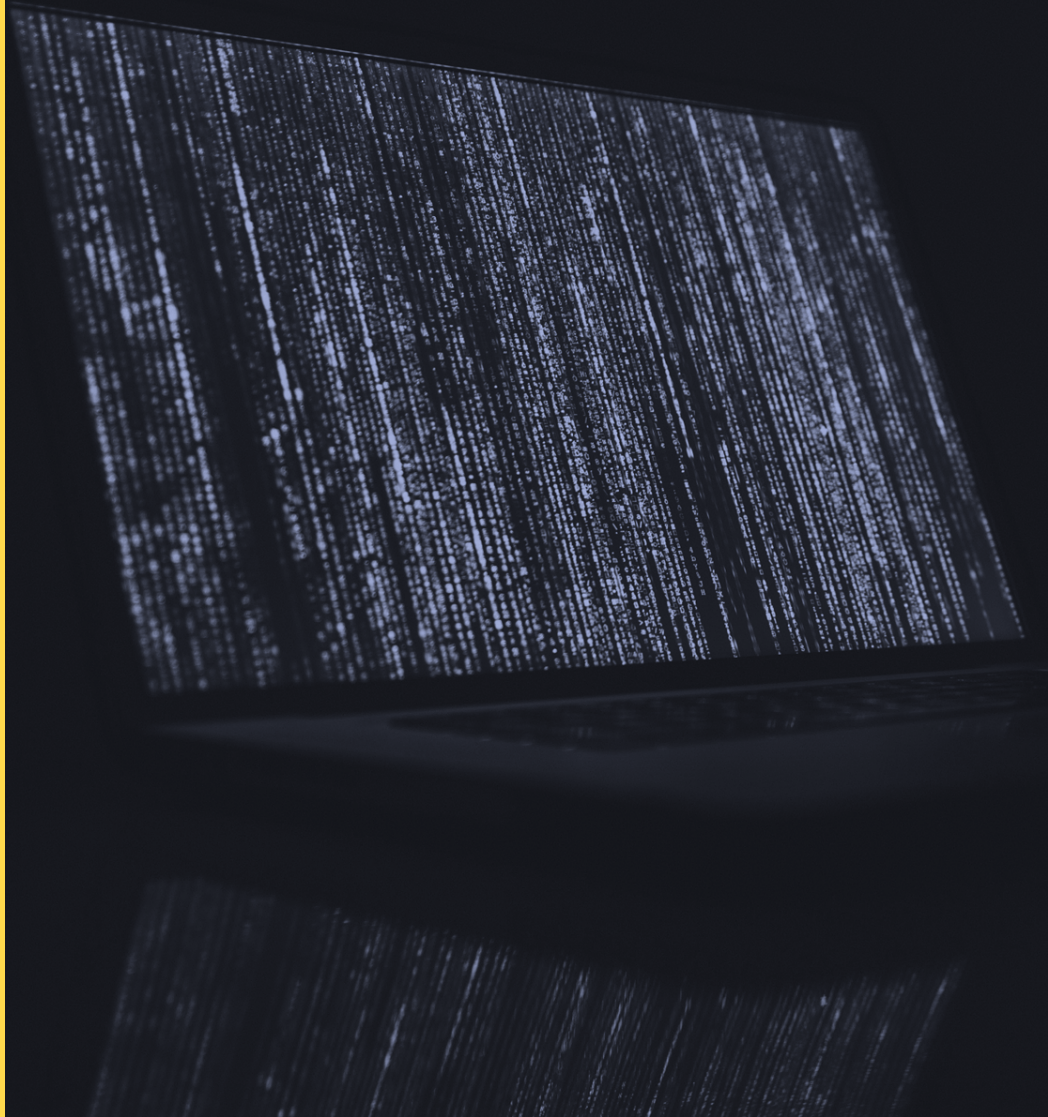
Back up your data

Regularly back up your data and make sure those backups are not connected to the network. That way, if a phishing attack happens and hackers get to your network, you can restore your data. Make data backup part of your routine business operations.



Alert your staff

Share with them this information. Keep in mind that phishing scammers change their tactics often, so make sure you include tips for spotting the latest phishing schemes in your regular training.



KEVIN MEKLER, ESQ.

Mullen Law | Chubb Cyber
Panel Counsel

Incident Response Stakeholders

The stakeholders and participants in the incident response (IR) process will vary depending upon the event, but may include some or all of the following parties:



The Victim Organization



Cyber Insurance Carrier/Broker



Incident Response Counsel/Breach Coach



Other Insurance Policy Carriers/Brokers, Such As K&R, Property, Crime, Etc.



Law Enforcement



Forensic Investigation and System Restoration Firm(s)



Extortion Negotiation and Payment Firm(s)



Data Mining Firm(s)



Other Legal Counsel (Depending on Specific Data Impacted and Applicable Regulatory Framework)



Public Relations Firm(s)



Notice Mailing and Call Center Provider(s)



Credit/Identity Monitoring Services



Insured Business Partner(s)

The (Potential) Incident Response Roadmap - Ransomware

Privileged Engagement of Forensic Investigation Firm

What happened? How did it happen? Is it ongoing? What is the impact and scope of interruption? What information may be at risk as a result of the event?

Engagement of Breach Coach/Notification to Carrier

Development of Communications Strategy

Engagement of Mailing, Call Center and Credit Monitoring Providers

Regulatory Interaction

Litigation/Claims

Single-Plaintiff; Class Action

Detection

Restoration

Backup v. Key

Mobilization of Incident Response Team

Notification to Law Enforcement

Engagement of PFI

For credit card events, as required

Engagement of Negotiation and Payment Firm

Engagement of PR Firm

Data Mining

Disclosures, As Required (Law, Contract, Courtesy)

Internal/External; Law Enforcement; Individuals; Regulators; Consumer Reporting Agencies; Media; Business Partners

RESOURCES

Knowbe4: <https://www.knowbe4.com/>

Free awareness training quizzes: <https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/quiz>

Data Privacy and Security Toolkit: <https://www.nar.realtor/data-privacy-security/nars-data-security-and-privacy-toolkit>


Cybersecurity Checklist: <https://www.nar.realtor/law-and-ethics/cybersecurity-checklist-best-practices-for-real-estate-professionals>

CHUBB RESOURCES

Legal > NAR Insurance Program

Cyber Resources


[Current Insurance Policy](#) [Employment Hotline](#) [Program FAQs](#) [NAR Policy Changes](#)

 Share

To complement the cyber liability and cyber response coverage in the NAR Insurance Program, Chubb offers access to enhanced benefits and services through various third party service providers to deliver extra assurance and specialized attention for their cyber policyholders.

If you have experienced a cyber incident, please call the Chubb Cyber Crisis Hotline 1-800-817-2665 for immediate assistance.

Chubb Panel Contact Information

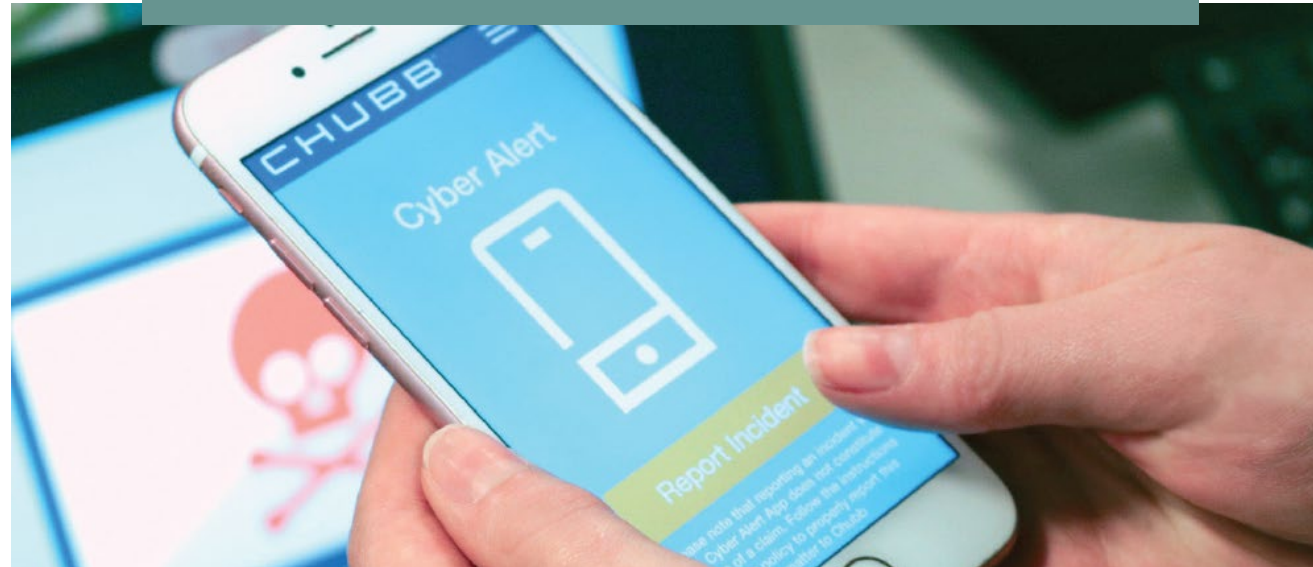
[Access Chubb's Cyber Partners for Mitigation and Response](#) 

Chubb has partnered with a panel of experienced firms for various cyber services related to incident response and loss mitigation. You may contact any of these providers for assistance with your cybersecurity program, however, you should conduct your own due diligence to ensure the provider and its services meet your needs. Unless otherwise approved by Chubb, payment for services provided by any provider is your responsibility.

<https://www.nar.realtor/legal/nar-insurance-program/cyber-resources>

Cyber Alert App

USE THE CHUBB APP



Chubb's Cyber Providers

Cyber Services

Chubb Panel Contact Information
North America




At Chubb, we believe that being prepared for a cyber incident can go a long way in limiting losses when one occurs. To complement our superior insurance protection, we offer access to enhanced benefits and services through various third party service providers to deliver extra assurance and specialized attention for our cyber policyholders.

Chubb has partnered with a panel of experienced firms for various cyber services related to incident response and loss mitigation.¹

Experience a Cyber Incident?

When you experience a cyber incident that you feel is an urgent matter, call 800-847-2665 or use the Chubb Cyber Alert® mobile application. The toll free number or mobile app will connect you to call center specialists to route the incident to one of our Response Coaches - pre-approved law firms that are adept in handling cyber matters.

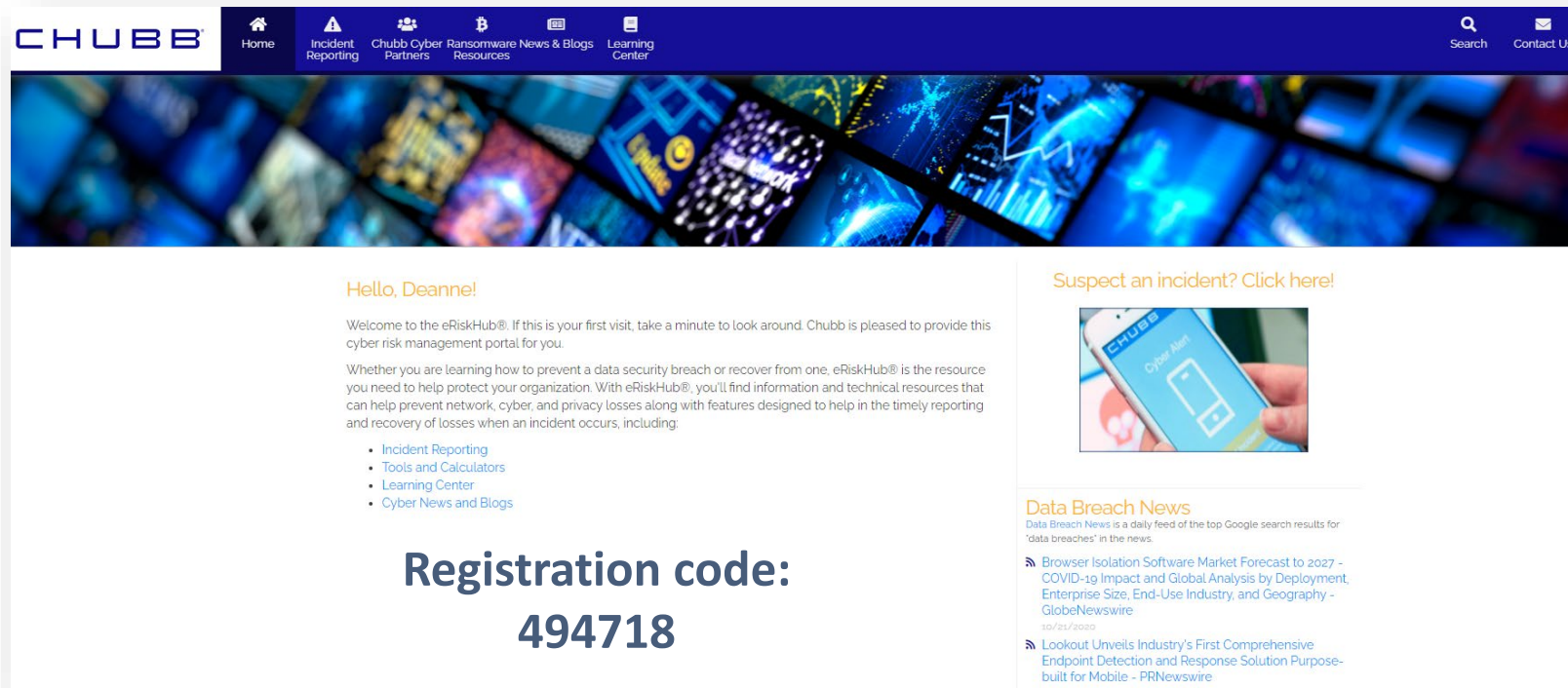
Incident Response Services: Partner Contacts

Company	Primary Service Capability	Contact Name	Phone	Email
BakerHostetler	Response Coach	Theodore J. Kobus III	(212) 271-1504	tkobus@bakerlaw.com
Borden Ladner Gervais	Response Coach (Canada)	Ira Nishisato	(844) 617-1887	inishisato@blg.com
Cipriani & Werner	Response Coach	Carolyn Purwin	(610) 567-0700	cpurwin@c-wlaw.com
Fasken Martineau	Response Coach (Canada)	Alex Cameron	(844) 200-7505	acameron@fasken.com
Marshall Dennehey	Response Coach	David J. Shannon	(215) 575-2615	djshannon@mdwvlg.com
Mullen Coughlin	Response Coach	John Mullen	(267) 930-4792	jmullen@mullen.legal
Norton Rose Fulbright	Response Coach	David J. Kessler (U.S.) Julie Himo (Canada)	(212) 318-3382 (514) 847-6017	david.kessler@nortonrosefulbright.com julie.himo@nortonrosefulbright.com

...	Notification			
...	Computer Forensics			
...	Computer Forensics (Canada)			
...	Computer Forensics			
...	Legal Counsel			
...	Computer Forensics			
...	Computer Forensics			
...	Computer Forensics			
...	Legal Counsel			
...	Public Relations			
...	Notification			
...	Notification (Canada)			
...	Notification			
...	Computer Forensics			
...	Computer Forensics			
...	Legal Counsel			
...	Legal Counsel	Thomas Bentz	202-828-1879	thomas.bentz@hklaw.com
...	Computer Forensics	Shawn Melito	(814) 207-4007	smelito@kivaconsulting.com

Loss Mitigation Services: Partner Contacts

Company	Primary Service Capability	Contact Name	Phone	Email
BitSight	Network Security	Samit Shah	(202) 215-6106	samit.shah@bitsighttech.com
Cofense	Security Education & Awareness	Robert Iannicello	(905) 505-0232	robert.iannicello@cofense.com
CrowdStrike	Endpoint Security	Charlie Groves	(303) 887-0506	charlie.groves@crowdstrike.com
Dashlane	User Account Security	Stewart Atkinson	(212) 596-7562	stewart@dashlane.com
Fidelis Cybersecurity	Response Planning	Rex Brunelli	(210) 366-6884	rex.brunelli@fidelissecurity.com
FireEye	Security Operations	Karen Kukoda	(916) 458-2030	karen.kukoda@fireeye.com
NetDiligence	Network Security	Dave Chatfield	(954) 684-9190	dave.chatfield@netdiligence.com
RSM	Compliance	Daimon Geopfert	(248) 802-4908	daimon.geopfert@rsmus.com
Skillbridge	Security Education & Awareness	John Lytle	(781) 466-6371	jlytle@skillbridgetraining.com
StealthBits	User Account Security	Brian Goodman	(610) 304-8064	brian.goodman@stealthbits.com
Thales e-Security	Data Security	Vincent Trovarelli	(609) 501-0343	vtrovarelli@thalessec.net



**Registration code:
494718**

www.eriskhub.com

NEXT WEBINAR



EMPLOYMENT LAW

December 8, 2022

2 pm CT

MORE INFORMATION

NAR INSURANCE PROGRAM

nar.realtor/nar-insurance-program

AON ACCOUNT EXECUTIVES

Gayle Andrews

Gayle.Andrews@aon.com

312-381-7049

Laura Sereika

Laura.Sereika@aon.com

312-381-2602

THANK YOU.



NARdotRealtor



nar.realtor

THAT'S WHO WE 

 NATIONAL
ASSOCIATION OF
REALTORS®