WOMEN AND THE LAW
STATE BAR OF TEXAS

# *Women and the LAW CLE and Wellness Retreat*

## *Tapatio Springs*

Boerne, Texas

*Elizabeth Cantu*
*Sofia A. Ramón*

RW
RAMÓN WORTHINGTON
LAW FIRM

# ATTORNEY BONDING OVER CYBER PROTECTION

**What will we discuss**

-general types of cyber threats

-regulatory and ethical obligations

-potential client requirements

-potential litigation

-best practices

-cyber insurance

**“Most cyberattacks are the result of**

**human error, with 90% vulnerabilities stemming from phishing emails.”**

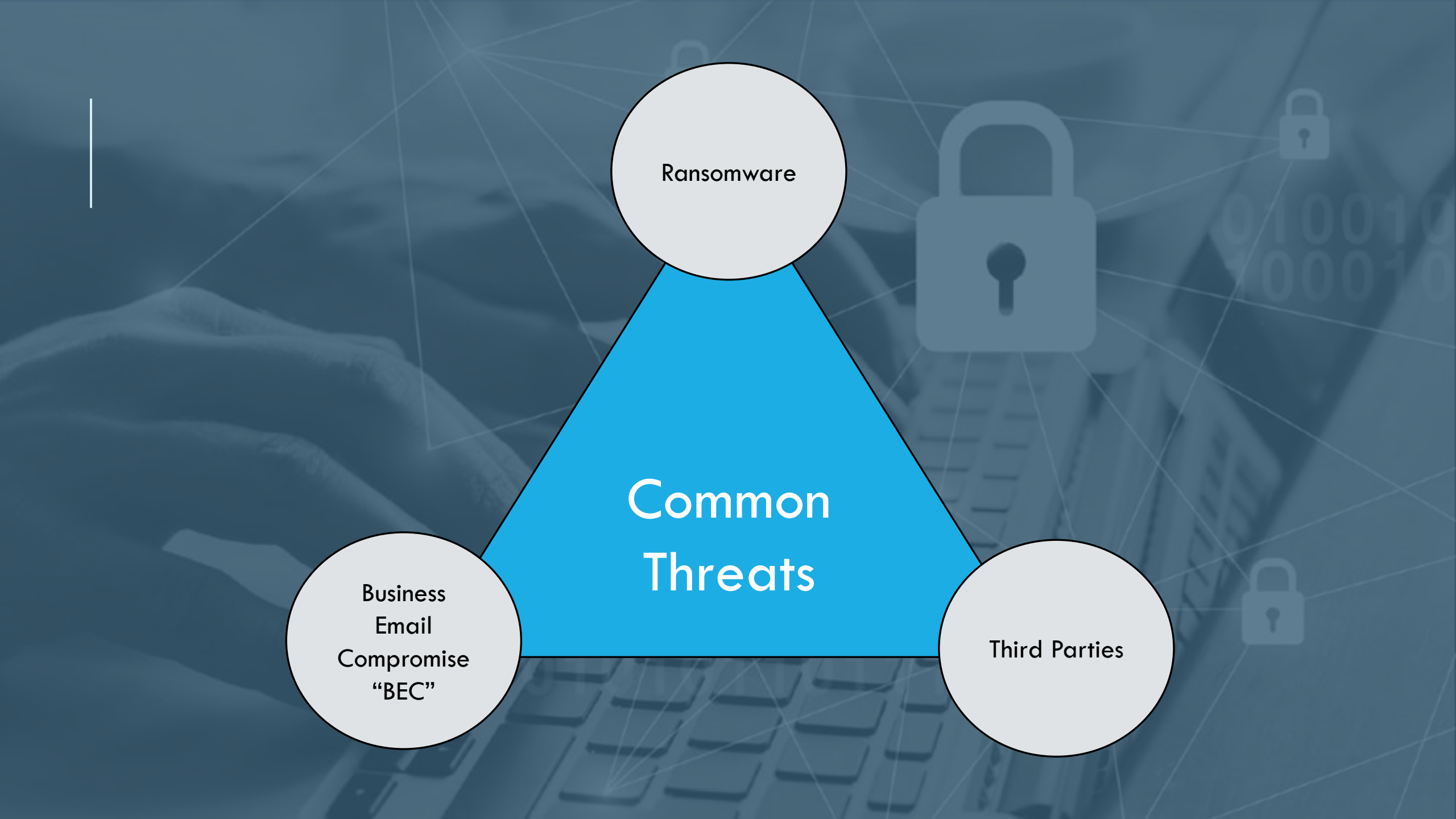
**-ABA TechReport 2022**

# SOME EXAMPLES OF DAMAGES CAUSED BY BREACHES

- DOWNTIME/LOSS OF BILLABLE HRS: 36%
- CONSULTING FEES FOR REPAIR: 31%
- DESTRUCTION/LOSS OF FILES: 13%
- REPLACEMENT OF HARDWARE/SOFTWARE: 18%
- REPORTED TO CLIENT: 24%

# WE DON'T NEED NO STINKIN' POLICY…!

- 53% have a policy to manage information retention and data;
- 60% have a policy on email use;
- 56% have a policy on internet use;
- 48% have a policy for social media use;
- 36% have a policy for personal computer use;
- 56% have a policy for their employees' own device;
- 57% have a policy for acceptable computer use;
- 56% have a policy for remote work;
- 44% have a policy for employee privacy; BUT
- 17% have NO POLICY at all; and
- 8% of firms reported not knowing their firms' policies.

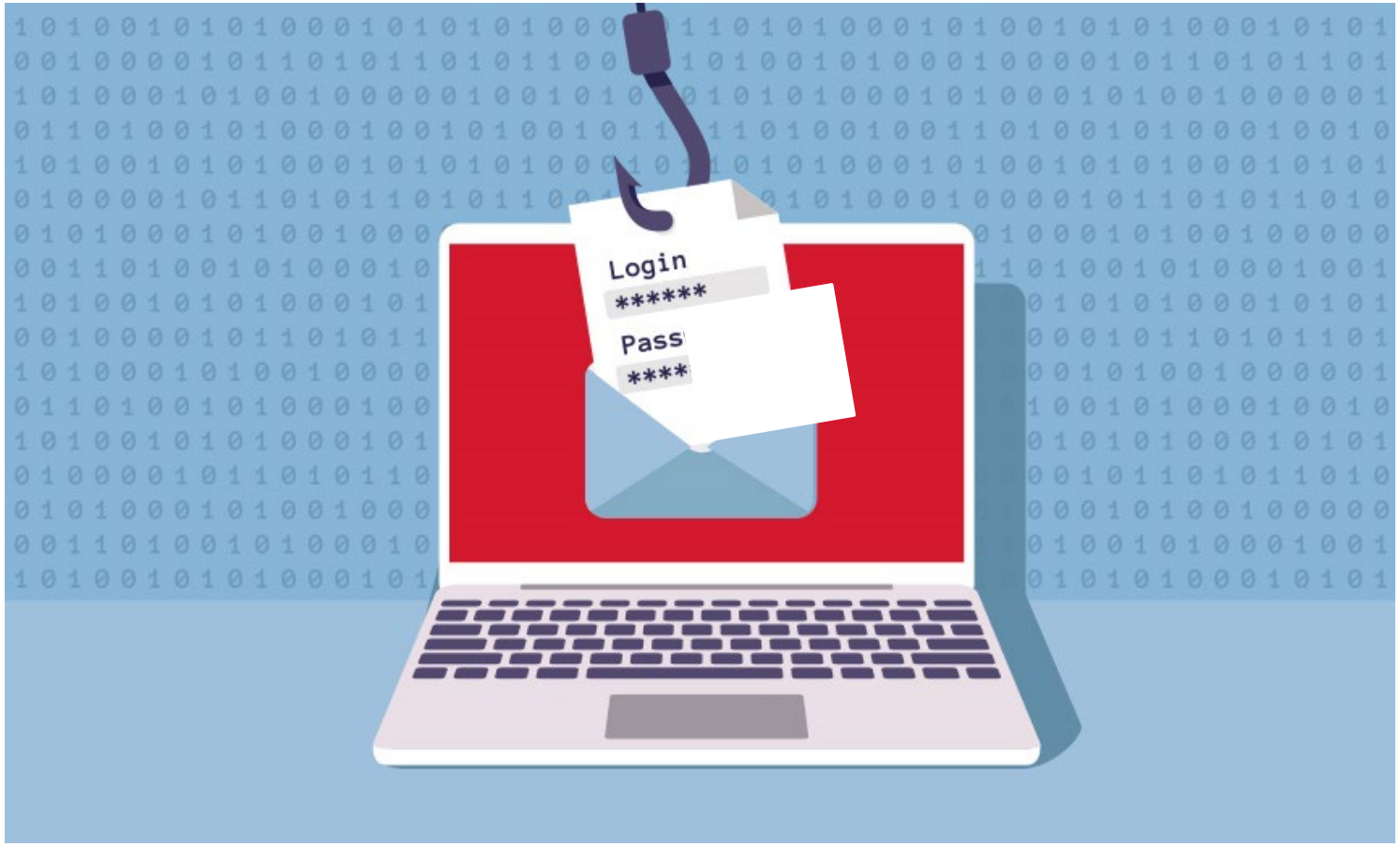

Ransomware
Common Threats
Business Email Compromise "BEC"
Third Parties

# RANSOMWARE

- Ransomware is a malware that encrypts your data with a digital key that only the bad actor has
- The data is held hostage until you pay the ransom and obtain the decryption key from the criminals
- Usually, criminals encrypt as much of a corporate network as possible to extort a bitcoin ransom in return for restoring the data

# BUSINESS EMAIL COMPROMISE

- A type of email cyber scam in which an attacker targets a business to defraud the company by posing as someone the recipient should trust



# BUSINESS EMAIL COMPROMISE

- CEO FRAUD
  - PRETEND TO BE CEO AND TARGETS FINANCE DEPARTMENT SEEKING FUNDS
- ACCOUNT COMPROMISE
  - E'ES ACCOUNT HACKED AND USED TO REQUEST PAYMENTS
- FALSE INVOICES
  - SCAMMER IMPERSONATES VENDORS AND REQUESTS PAYMENT TO FRAUDULENT ACCOUNTS

# How Domain Spoofing Works

A Hacker performs a deep search for your organization's email addresses

They locate all available employee email addresses

They target these users making it appear their email comes from a trusted source

**From:** Slater C. Elza
**To:** Sofia Ramon
**Subject:** Expense Disbursement
**Date:** Friday, December 4, 2020 9:17:06 AM

---

[EXTERNAL]

Hi Sofia,

What's your schedule for today? I need you to handle a payment request for me today. send me an email back if you can help out so i can provide you the payment details needed.

Thanks
Slater C. Elza

**From:** Douglas Rees
**To:** Sofia Ramon
**Subject:** Sofia
**Date:** Monday, April 3, 2023 12:03:32 PM

---

[EXTERNAL]

I presently have limited phone access because I'm not in the office. Will you be able to take care of our operating (networking activities, website hosting) and program services expenses? which is due, on our behalf?

Darin Brooks is not available to complete it right away, If you can pay for it through Zelle, please let me know so I can forward you the vendor's Zelle payment details. I will process your reimbursement by the end of the day.

Best regards
Douglas Rees

Sent from my iPhone

WHAT JUST HAPPENED?

# THE ETHICS

# DON'T ASK, DON'T TELL?

**WRONG!**

LAW FIRMS ARE SUBJECT TO REPORTING AND NOTICE REQUIREMENTS FROM SEVERAL SOURCES…these are a few:

- ***TEXAS RULES OF PROFESSIONAL CONDUCT RULE 1.05(b)***
- ***ABA MODEL RULES, RULE 1.6 ( c ) and Rule 1.1***
- ***TEXAS DATA BREACH NOTIFICATION LAW, TEX.BUS.&COMM.CODE 521.053***
- ***TEXAS MEDICAL RECORDS PRIVACY ACT ("TMRPA"***
- ***HIPAA***

# DON'T FORGET CLIENT GUIDELINES!

**"Please remember that pursuant to the Engagement Guidelines you must notify insurance company as soon as possible, but no later than, twenty-four (24) hours after becoming aware of any potential security incident, data breach, cybersecurity event, or any other event that impacts or has the potential to impact insurance company's confidential information. Notice should be made to Insuranceco@insuranceco.com or by telephoning (000) 000-0000."**

The Firm shall encrypt all electronically stored client Confidential Information in its possession both at rest and in transit.

"If the Firm does not have the in-house capability to perform the actions required by this Section in a professional and competent manner, the Firm shall retain an outside forensic expert to do so at the Firm's own expense. All loss of information or knowledge, or of the reliability thereof, caused by the Firm's failure to retain an independent qualified forensics expert shall be presumed to be the fault of the Firm."

What does your client require?
Do you have a “Response Plan”

**The Firm’s Security Program shall include a “Response Plan” which shall consist of implemented policies and procedures to address a Security Event (defined below) by mitigating the harmful effects of Security Events and addressing and remedying the occurrence to prevent the recurrence of Security Events in the future.**

# Would you agree??

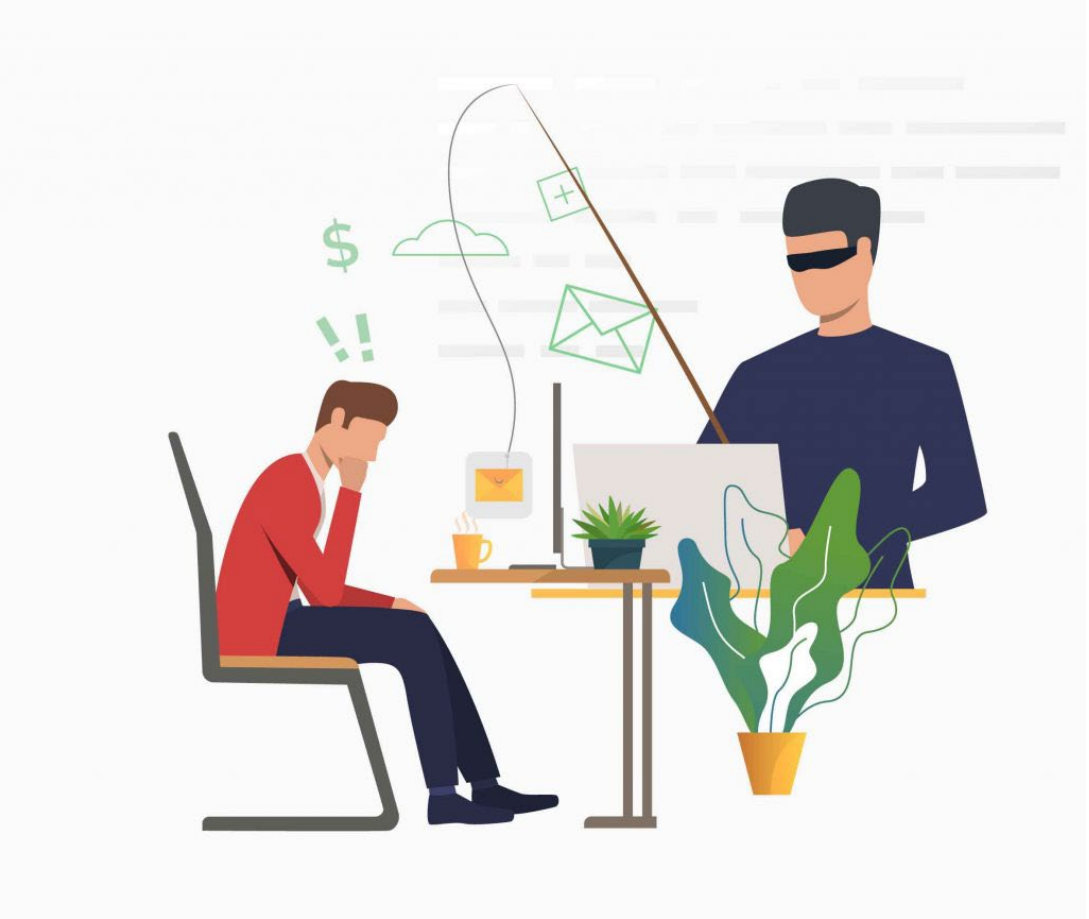
To the fullest extent permitted by law, the Firm hereby waives the benefit of any state or federal law which may provide a cause of action against client based on actions permitted under this Section.

# WHAT TYPE OF LITIGATION CAN ENSURE

# WIRE FRAUD

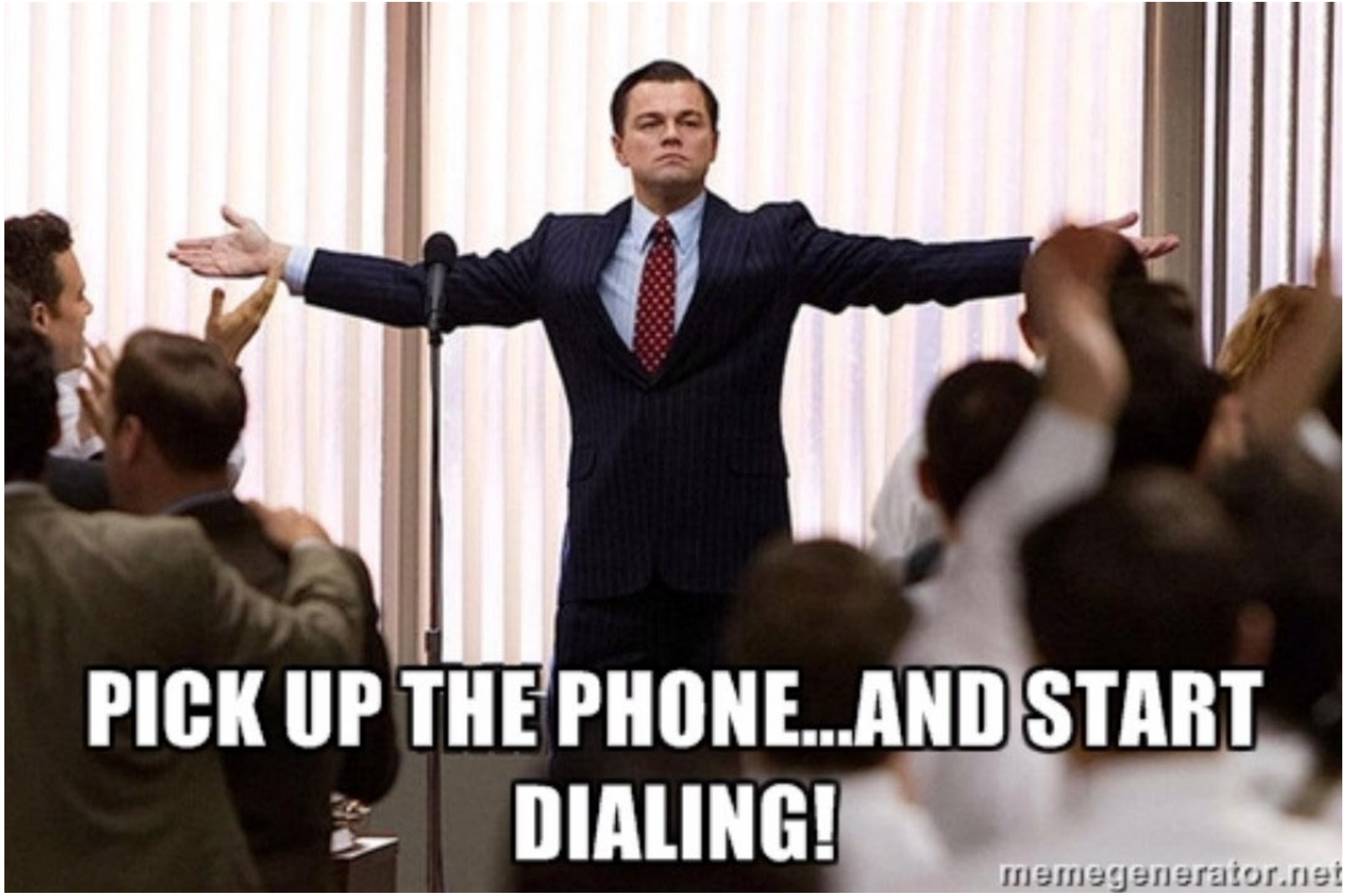
- Bile v. RREMC, LLC (2016)
- Arrow Truck Sales. Inc. v. Top Quality Truck & Equip. Inc.
- J.F. Nut Co. v. San Saba Pecan (2018)
- Jetcrete N. Am. LP v. Austin Truck & Equip., Ltd. (2020)
- Peeples v. Caroline Container (2021)

- The “Imposter Rule”
- Utilized analysis set out in UCC 3-404, and restated that the party who was in the best position to prevent the forgery, by exercising reasonable care, suffers the loss



# CLASS ACTION LITIGATION

# HOW TO PROTECT YOURSELF AND YOUR CLIENTS


PICK UP THE PHONE...AND START DIALING!
memegenerator.net

## Best Practices

| | |
|---|---|
| Two Factor Authentication | |
| Call to confirm wire instructions | |
| Have strong and unique passwords | Change them frequently! |
| Look at your forwarding rules | This is to determine whether there is an outbound email traffic to an unknown account from your account. If so, disable those forwarding rules and change your password |
| Train your employees about scams | |
| Use encryption for files | |

| | |
|---|---|
| **Best Practices** | Activate find device and remote wipe on mobile devices |
| | Use antivirus and antimalware protection |
| | Update security software |
| | Don’t use personal email accounts on business computers |
| | Do not connect to unknown Wi-Fi networks |
| | Secure your internet connection with a firewall. |

# IS THERE INSURANCE TO PROTECT YOU AND YOUR CLIENT?

# Cybersecurity Insurance




## What are the types of cybersecurity coverage?

First-party coverage

Third-party or cyber liability coverage

Technology errors and omissions

## What does cybersecurity insurance exclude?

Property damage.

Intellectual property.

Crimes or self-inflicted cyber incidents.

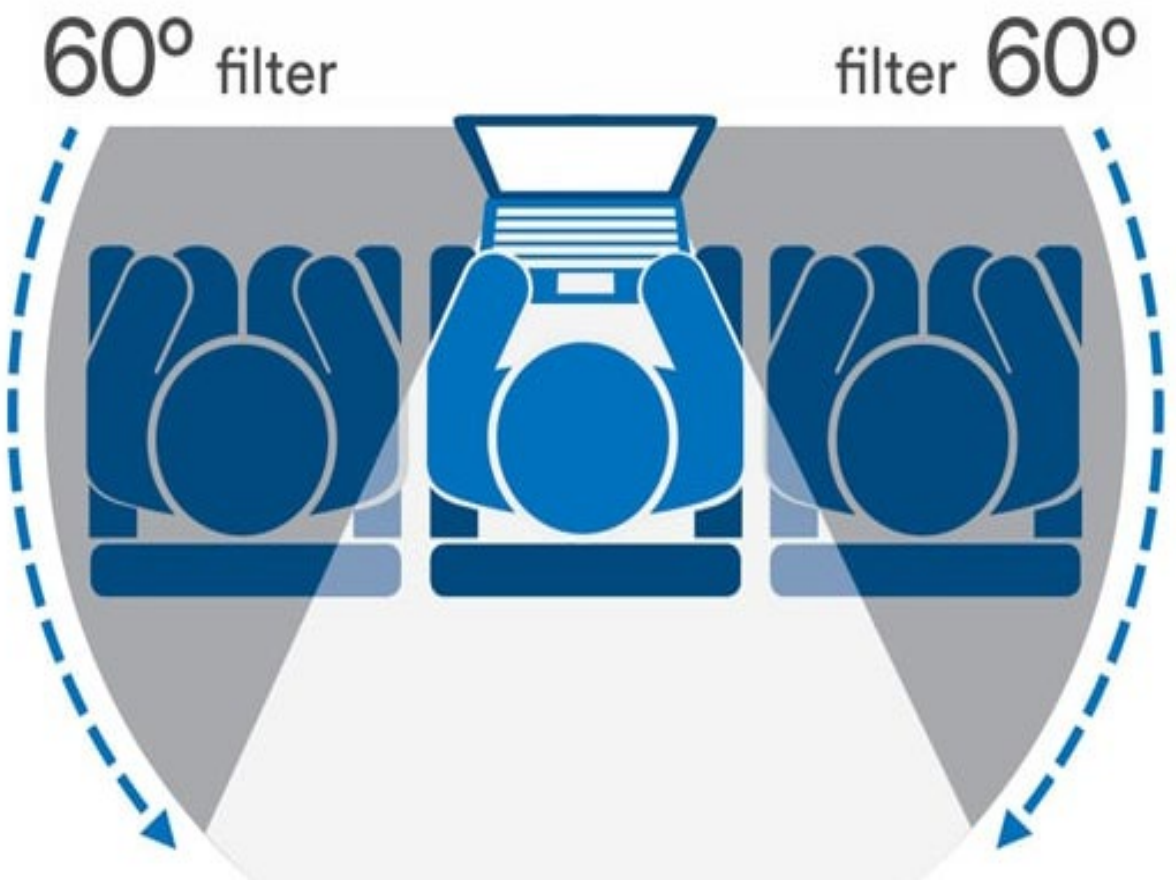
Costs for proactive preventive measures.


# VPN

- Hides your IP address, location, and all digital activities, including downloads.
- VPN protects your activity so any hacker or malicious actor on the same network as you will not be able to see the information transmitted to and from your device.

# PROTECT YOUR INFORMATION

Privacy Screens for Phones and Computers



# FIRST-PARTY VS. THIRD-PARTY CYBER INSURANCE

## First-Party

First-party cyber liability insurance protects your company. It will cover all of the costs related to a cyberattack, including but not limited to the following:

- Forensic analysis for identifying the attack source
- Public relations services
- Notification of clients
- Credit monitoring services
- Loss of income

## Third-Party

Third-party cyber liability insurance is tailored towards providing protection for businesses that offer professional services to other businesses that can be compromised by cyberthreats.

- For example, if your law firm's data security is compromised, and your law firm is accused of failing to prevent the data breach, third-party cyber liability insurance can pay legal fees, government penalties and fines, and settlements and judgments related to such claims.

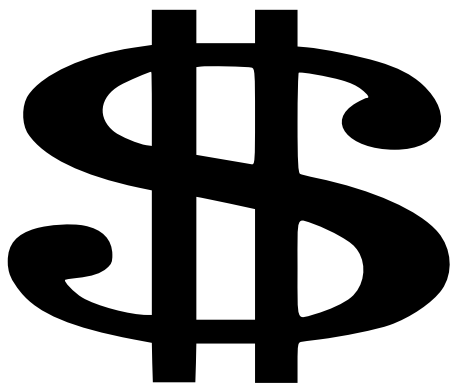
# RANGE OF PREMIUM COSTS

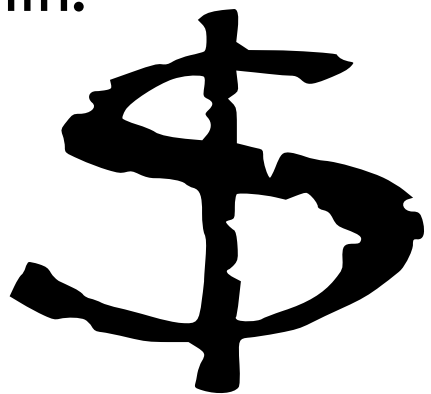
Factors affecting premium costs

1. Size and Industry
2. Amount and Sensitivity of Data
3. Annual Revenue
4. Strength of Security Measures
5. Policy Terms

The average cost of cyber insurance in the U.S. in 2021 was $1,589 per year or $132 per month.

The average cost of cyber insurance for Law Firms in 2021 was $2,269 per year or $189 per month.






# SAMPLE QUESTIONS FOR CYBER INSURANCE APPLICATIONS

- Do You Use Multi-Factor Authentication (MFA)?
- Do You Provide Employee Security Training?
- Do You Monitor For Unauthorized Access?
- Do You Back Up Your Data?
- Do You Have Endpoint Protection?
- Do You Use Encryption?
- Do You Limit Access To Data & Systems?
- How Do You Install Updates & Patches?
- Do You Have A Disaster Recovery Plan?


The Hartford Steam Boiler Inspection and Insurance Company (HSB)

- Coverage for cyber extortion and misdirected payments
- Limits as low as $50,000
- Access to risk management tools and training modules


- If something unfortunate happens like a data breach Liberty Mutual will:

•Notify your customers about the data breach

•Comply with regulatory proceedings

•Pay cyber extortion ransoms


- They have customizable plans that you can tailor to your company size, even if you're only collecting data from a handful of customers or employees.
- If you're already using Progressive for business or general liability coverage, you can add cyber insurance coverage.




Elizabeth Cantu
ecantu@ramonworthington.com
Sofia A. Ramón
sramon@ramonworthington.com