

OSB Professional Liability Fund presents

# Understanding Your Firm's Cybersecurity Obligations and Exposures

Wednesday, May 31, 2023

10:00 am – 11:00 am

MCLE ID 98884

.5 Ethics Credit, .5 PS Credit

Speakers: **Hong Dao**  
*Director of Practice Management Assistance Program, PLF*

**Sarah Dufendach**  
*Cyber Claims Manager, Beazley Group*



Professional  
Liability Fund

## CLE Materials

- PowerPoint Slides
- Oregon Rules of Professional Conduct,  
<https://www.osbar.org/docs/rulesregs/orpc.pdf>
- ABA Formal Opinion 498,  
[https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/aba-formal-opinion-498.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba-formal-opinion-498.pdf)
- ABA 2022 Legal Technology Survey Report (summaries),  
[https://www.americanbar.org/groups/law\\_practice/publications/techreport/2022/cybersecurity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2022/cybersecurity/)
- Verizon 2022 Data Breach Investigative Report,  
<https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/>
- PLF Practice Aids on Cybersecurity and Data Breach, available at:  
<https://www.osbplf.org/services/resources/#forms> or go to our website:  
[www.osbplf.org](http://www.osbplf.org) > Services > CLEs & Resources > Practice Aids



# UNDERSTANDING YOUR FIRM'S CYBERSECURITY OBLIGATIONS AND EXPOSURES

Presented by

Hong Dao, Director of Practice Management Assistance Program, OSB PLF  
Sarah Dufendach, Claims Manager, Beazley

# Why are lawyers and law firms target?

- Warehouses of valuable data
- Security vulnerabilities
- Conduct large financial transactions

```
renderHeaderFooterDetailsCard() {
```

```
renderContainer() {
```

```
renderFooter() {
```

```
renderFooter() {
```

```
renderFooter() {
```


```
renderFooter() {
```

```
143     >
144     Instagram
145     </div>
146   </div>
147   </div>
148   </div>
149   }
150 }
151
152 *
153 *
154 *
155 *
156 *
157 *
158 *
159 *
160 *
161 *
162 *
163 *
164 *
165 *
166 *
167 *
168 *
169 *
170 *
171 *
172 *
173 *
174 *
175 *
176 *
177 *
178 *
179 *
180 *
181 *
182 *
183 *
184 *
185 *
186 *
187 *
188 *
189 *
190 *
191 *
192 *
193 *
194 *
195 *
196 *
197 *
198 *
199 *
200 *
201 *
202 *
203 *
204 *
205 *
206 *
207 *
208 *
209 *
210 *
211 *
212 *
213 *
214 *
215 *
216 *
217 *
218 *
219 *
220 *
221 *
222 *
223 *
224 *
225 *
226 *
227 *
228 *
229 *
230 *
231 *
232 *
233 *
234 *
235 *
236 *
237 *
238 *
239 *
240 *
```



# Lawyer's Ethical Obligations

---

- 
- ORPC 1.6 – Protect confidentiality
  - ORPC 1.1 – Provide competent representation
  - ORPC 1.4 – Communicate with clients
  - OSB Formal Ethics Opinion 2011-187 – Understand technology and its risks
  - ORPC 5.1, 5.2, and 5.3 – Duty to supervise
  - (ABA Formal Opinion 498 (3/10/21))

# Cybersecurity landscape for law firms

## ABA's 2022 Legal Technology Survey Report

- 68% - stayed abreast of the benefits and risks of technology
- 75% - had training (32% of solos, 64% for 2-9 atty firms, 79% for 10-49 atty firms , 93% 50-99 atty firms and 100% for 100+ atty firms)

## Firms experiencing security breach:

- 27% - YES
- 25% - didn't know (5% for solos, 12% for of 2-9 atty firms, 25% for 10-49 atty firms, 33% for 50-99 atty firms and 50% for 100+ atty firms)
- 48% - NO



# Types of Cyber Threats

---

# Law Firm Threats

- Ransomware/Cyber Extortion
- Business Email Compromise
- Fraudulent Instruction





# Ransomware/Cyber Extortion



Phishing



Remote Desktop  
Protocol (RDP)

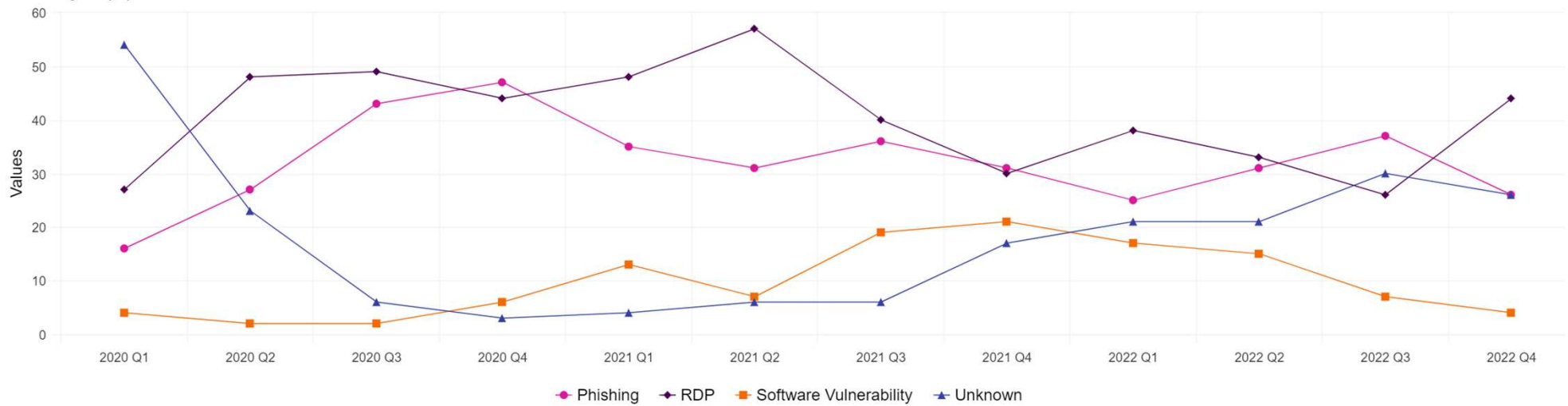


Software/Hardware  
Vulnerabilities

# Ransomware Vectors

## Ransomware vectors

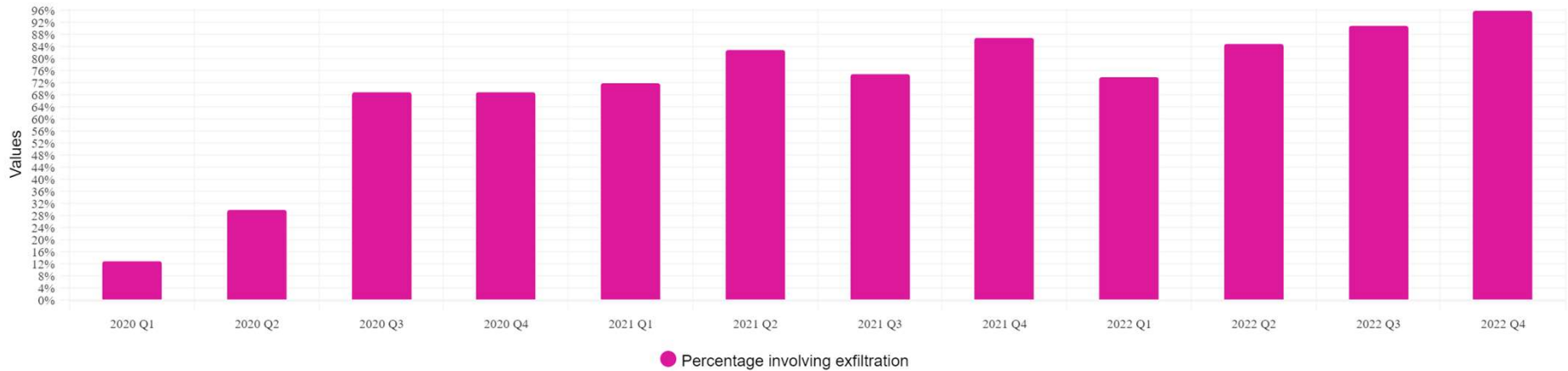
Percentages by quarter



# Ransomware/Cyber Extortion

## Cyber Extortion Incidents with Data Exfiltration

Percentages by quarter



Over the course of 2022, we have observed data exfiltration becoming solidly a part of the threat actor's playbook, to such an extent that only one cyber extortion event in Q4 did not involve threat of exfiltration. For more on this trend and its ramifications, see our earlier report on [Examining Data Exfiltration](#).

# Ransomware Scenario

## 1. Initial compromise of your environment

### Remote Access Security

- Microsoft RDP and Remote Desktop Gateway (RDG) can be used to provide remote access to computers and networks.
- RDP/RDG attacks are an attractive and common way for hackers to access systems and steal valuable information from devices and networks.

### Phishing

## 2. Malware is installed

- The user opens the attachment and malware is unknowingly installed on the user's PC.
- Unbeknownst to the user, and your security and IT teams, the attackers now have a foothold in your environment.
- Using this foothold, the hackers explore your network (still undetected) looking for vulnerable systems and sensitive data. This includes other users' PCs but also servers supporting critical applications and file stores.

## 3. Ransomware is deployed

- The criminal group has achieved the access they need and are ready to spring their trap.
- They deploy a strain of ransomware which spreads across your network encrypting indiscriminately.
- The attackers have now encrypted a material portion of your estate and parts of your business are completely disrupted while other parts are partially disrupted.

## 4. Extortion

- The attackers demand \$x million for the decryption key.
- The attack also becomes public knowledge which causes reputational damage.
- The regulator also wants to understand if there has been a mishandling of customer sensitive data – there is a risk of a significant fine.

# Avoid Phishing Tips

---

- Train yourself and staff to identify phishing emails
- Change email view
- Use spam filters
- Use secure client portals
- Advise clients early on re communications





# Remote Desktop Protocol (RDP) Tips

- Disable RDP altogether if you do not need or use it
- Use current versions of Windows and regularly update and patch
- Enforce a strong password policy with regular password changes
- Allow RDP access to only those networks and accounts that actually need it
- Use a VPN with MFA if you do use RDP

# Business Email Compromise

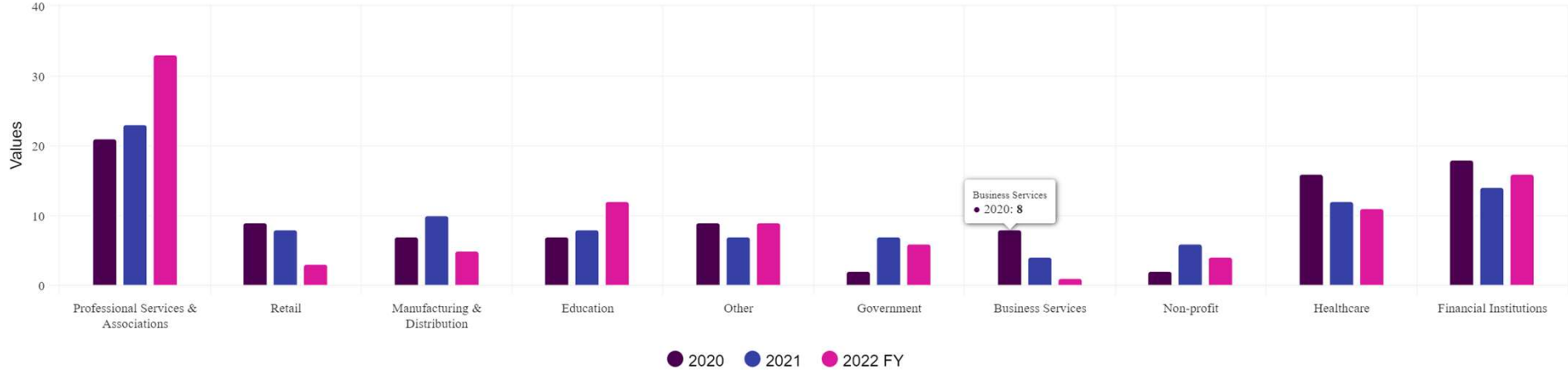
- Phishing/Compromised Credentials
- Lack of MFA
- Unpatched Vulnerabilities



# Business Email Compromise

## Business Email Compromise

Percentages by Industry



While business email compromise has declined overall in 2022, professional services and education both grew from 2021. Both industries are running notably ahead of where we'd expect, with financial institutions not far behind. Watch for this trend to continue in 2023.



# Implement Multi-Factor Authentication (MFA)

---

More secure forms of MFA:

- Push notifications
- Time-based one-time passwords (TOTP)
- OAuth (Open Authorization) tokens
- Hardware tokens, authenticator apps
- Biometrics
- FIDO2 key like YubiKey or RSA SecurID



# Fraudulent Instruction

- Business Email Compromise
- Phishing/Spoofed Emails
- Failure to Out of Band Authenticate

## Scenario 1—Our system has been breached, and someone's email account has been hacked

In this scenario a hacker has gained access to our systems and is able to hijack our email accounts. This means that they have a co-worker's credentials and can be communicating with you without the co-worker having any idea their email is being used. The result is "your co-worker" sending you an email with fraudulent instructions. Often in these cases the attackers will monitor our communications for a while and use information discovered that way to send a more convincing email.

## Scenario 2—Vendor's system has been hacked

In this scenario, one of our vendors has been hacked, and the attacker sends you an email from the vendor's account asking you to send money. Like in the first scenario, the email will be from a legitimate account of someone you have communicated with in the past. The attacker will also likely monitor communications and jump in after legitimate emails have been sent back and forth so that it looks like a continuation of your conversation with the vendor.

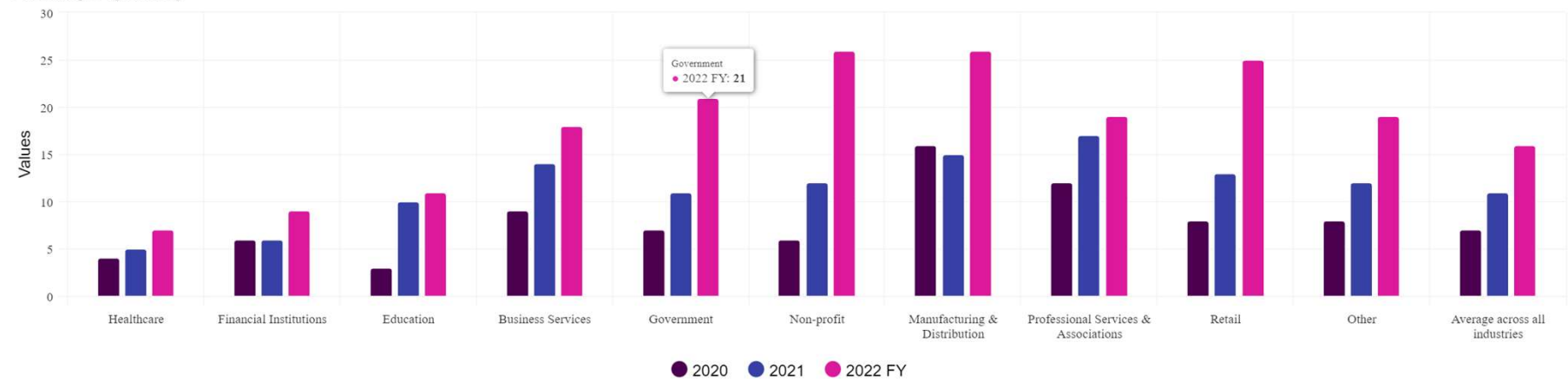
## Scenario 3—Vendor's email is spoofed

This scenario is different than the first two because nobody had been "hacked." Instead, the attacker just makes it look like they are one of our vendors. Attackers are smart, so the email will look similar to what our actual vendor's email would look like. They may copy the logo. The email address will likely be only off by one or two characters. An example is *CEO@company\_xyz.com* vs. *CEO@company-xyz.com*.

# Fraudulent Instruction

## Fraudulent Instruction as a Cause of Loss

Percentages by industry



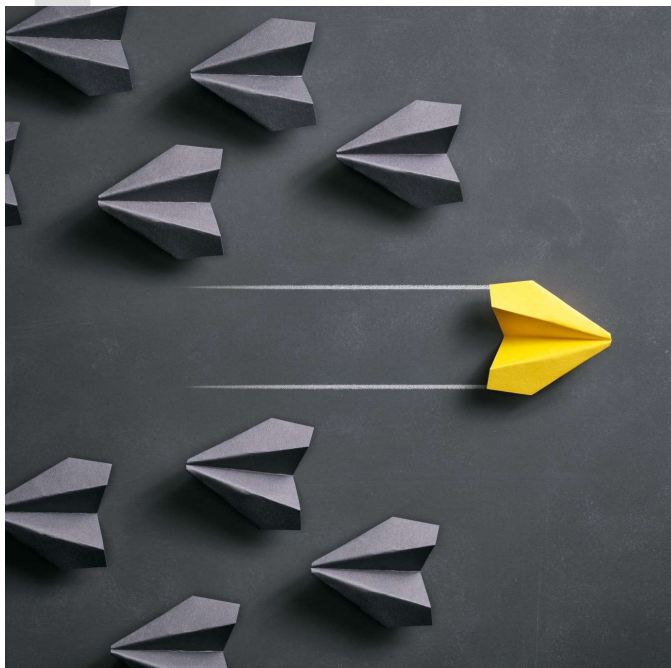
As a category, fraudulent instruction experienced big growth as a cause of loss in 2022, up 13% year-over-year. This trend continues to be quite high compared to where we would expect it to be, especially when it comes to small business.

# Out of Band Authentication

- Protect from fraudulent instruction loss
- Verify any new payment requests through a different mode of communication than it came through
- Harder for an attacker to impersonate someone trusted through two modes than through one

## Examples:

- You get an *email* from a vendor → *call them* using the number you previously had on file *and confirm* that they sent the email.
- You get an *email from a co-worker* asking to send money to a new vendor or changes the account information for an existing vendor, *check it out* → Walk to their workspace or call them on their extension to confirm.



# Other Tips



Back up data  
and segment  
backups



Keep software  
patched and  
maintained



Train  
employees on  
best security  
practices



Implement  
Endpoint  
Detection &  
Response  
(EDR)



Conduct  
vendor due  
diligence

# Online Cybersecurity Employee Training Courses

- BrightWise (<https://www.bright-wise.com>)
- Inspired eLearning (<https://inspiredelearning.com>)
- KnowBe4 (<https://www.knowbe4.com>)
- Proofpoint (<https://www.wombatsecurity.com>)
- Webroot (<https://www.webroot.com/us/en/business/security-awareness>)



# What to do after a cyber security incident?



Implement IRP



Call people on IRP contact list



Immediately report to your insurer

Determine  
the  
following:

Scope nature and  
scope (digital  
forensics)

What data is  
affected (digital  
forensics and data  
breach lawyer)

If data is  
compromised  
(digital forensics and  
data breach lawyer)

If clients need to be  
notified (ethics/data  
breach lawyer)

If other entities need  
to be notified  
(ethics/data breach  
lawyer)

Liability exposure  
(PLF, cyber insurer)

Remedial actions  
(digital forensics)

---





# Cyber Coverage Response

---

# Cyber Coverage

- **Breach Response Manager**
  - Immediately responds to the incident
  - Reaches out to the insured to put together a plan of action
  - Connects insured to digital forensic investigator, privacy counsel, and ransomware consultant
- **Forensics**
  - Helps determine how a bad actor got into insured's system
  - Tracks their movements and helps contain incident
- **Privacy counsel**
  - Works with the insured and forensics to help insured determine liability
  - If notifications are necessary, privacy counsel assists with drafting notifications
- **First Party coverages**
  - Reimburse the insured for cyber extortion loss, data recovery costs and business interruption loss
- **Third party coverages**
  - Defend the insured against individual or class action lawsuits as well as regulatory inquiries and pays damages or penalties

---

# PLF Coverage

---

## PLF Primary Coverage

- Covers claims arising from the private practice of law
- DOES NOT cover cyber claims

## PLF Excess Coverage

- Covers cyber claims



An aerial photograph of a multi-lane highway bridge spanning across a body of turquoise water. The bridge has several lanes in each direction, with a few vehicles visible. A large, light gray circle is overlaid on the left side of the image, partially covering the bridge and the water. The text "Thank you!" is centered within this circle.

Thank you!