WEBINAR

CYBERSECURITY:

PROTECT YOUR DIGITAL ASSETS & ONLINE PRESENCE

CONTINUING EDUCATION AIA

▶ Wednesday, March 8, 2023

PRESENTER: **Tony Whitledge**, Cybercrime Expert
Whitledge & Company LLC

PUA

Arch

Construction Risk

Meet PUA

WHEN IT COMES TO PROFESSIONAL LIABILITY

WE'RE THE PROFESSIONALS

Four lines:

- A&E
- Design/build contractors
- MISC
- Excess

Strong paper & broad coverage

- Arch – admitted
- Lloyds – E&S

Stability and proven track record

Unparalleled underwriting expertise

Assist in navigating difficult, complex risks and issues

- **NEW!** PUA Market Solutions

Excellent claims support, in-house claims team

AIA Registered Course

This course is taught by a Registered Provider with The American Institute of Architects Continuing Education Systems. Credit earned on completion of this program will be reported to CES Records for AIA members. Certificates of Completion for non-AIA members are available on request.

This program is registered with the AIA/CES for continuing professional education. As such, it does not include content that may be deemed or construed to be an approval or endorsement by the AIA of any material of construction or any method or manner of handling, using, distributing or dealing in any material or product. Questions related to specific materials, methods, and services will be addressed at the conclusion of this presentation.

Copyright Information © 2023

Lessons Learned

- Understand the risks to our online privacy and security
- Explore our tolerance for risk and our level of concern for our own privacy
- Develop a strategy to improve our risk levels based on our level of concern and willingness to take affirmative action to protect against those risks
- Talk about your obligations to protect business data and networks when:
  - You are using company-provided devices (computers, phones, tablets, etc.)
  - You are using your own devices to access company resources (“BYOD”)

Online Privacy and Security

Why Do You Care? (Part 1)

- Privacy is keeping information about you to yourself
- Why do you care?
- Levels of concern about privacy
  - I'm good, nothing to hide, I want people to know where I am and what I'm doing
  - I don't want information about me out there, but I'm not going to make much of an effort to protect it
  - I value my privacy enough to take reasonable and ongoing steps to protect it
  - I'm a very private person and I'll do whatever it takes for as long as it takes to protect my privacy

Online Privacy and Security

Why Do You Care? (Part 2)

- Security is protecting your assets and information from outsiders
- You care because your security protects the money in your bank account, your credit card information, and your identity
  - Levels of concern about online security
    - I'm good; I trust the banks, card issuers, and others to protect my assets and identity
    - I want to keep everything secure, but I'm not willing to go to much effort
    - I'm willing to take reasonable and ongoing protective steps
    - I'll do whatever it takes for as long as it takes to protect my assets and my identity

Online Privacy

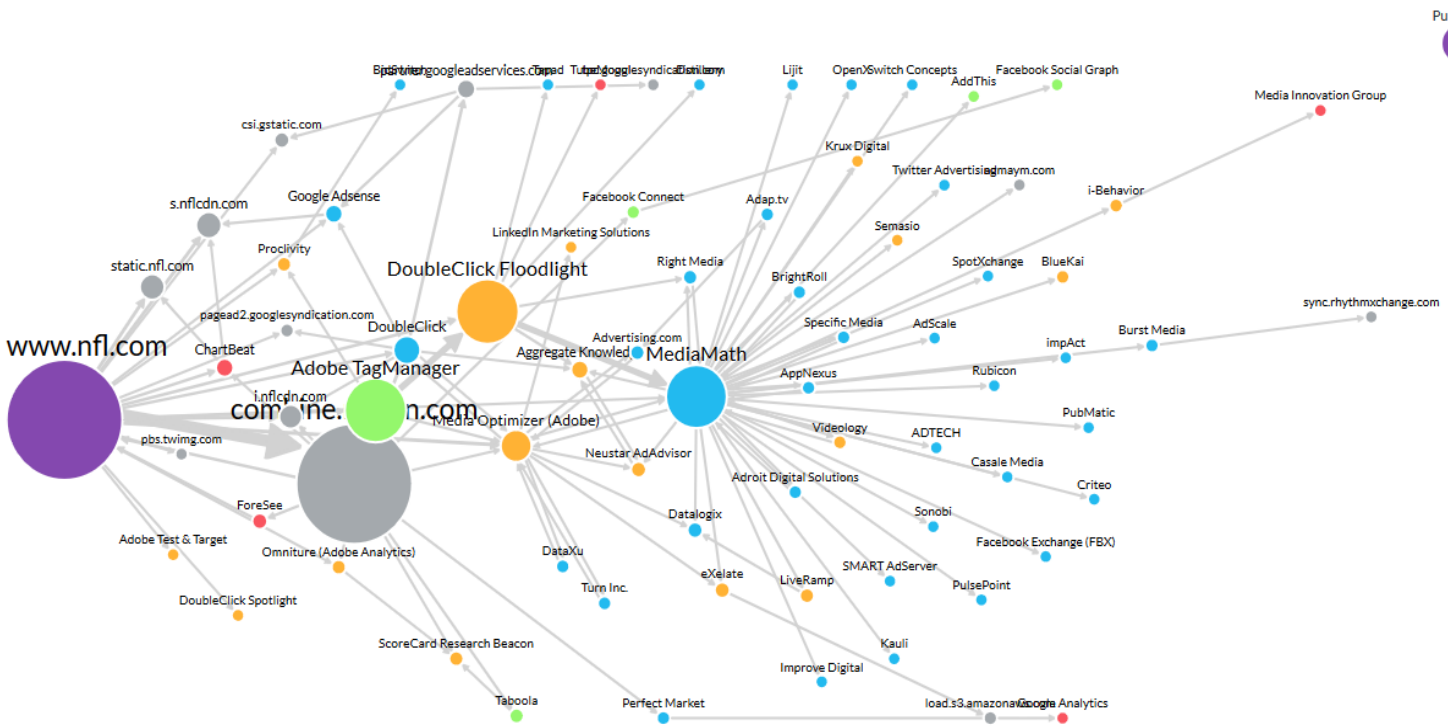
- Surveillance is the business model of the Internet
  - You get free access to sites and services in exchange for giving up your privacy and personal information
  - Everyone is collecting (and making money from) your personal information, including your physical location
    - ISPs
    - Microsoft, Google, Apple
    - Social media sites
    - Merchants
    - Advertisers and data aggregators

The Myth of Online Privacy

- There is no online privacy for individuals
- Data aggregators collect every online transaction and build personally identifiable databases about your life and habits
  - Targeted advertising is a multi-billion-dollar business
  - Many, if not most, of the websites you visit get paid to allow data aggregators to collect information from you
  - Example on next slide

GHOSTERY ENTERPRISE

TrackerMap | Timeline | Tree



How Do They Do That?
Web bugs, you say, what's a web bug?

- A 1 pixel x 1 pixel "GIF" image embedded in web page code
  - Directs the user to send information to, usually, a third-party Internet marketing company (i.e., doubleclick.com)
  - Sends user's IP address, browser type, site user visiting, time, etc.
  - By collecting web bugs, advertisers can build a profile of each user by matching identifying information from sites the user visits
  - Advertisers do not disclose use of web bugs to users
    - Is that legal? Good question

Is There Any Way to Prevent Targeting? (Part 1)

- You can't eliminate that targeting, but you can minimize it
  - If you **are Level 0** ("I'm good"), never mind
  - **Level 1** – One time shot to minimize data collection
    - Use more secure browsers and search engines
      - Firefox, Opera, Brave, Tor, etc.
      - Change default search engine to DuckDuckGo

Is There Any Way to Prevent Targeting? (Part 2)

Level 1 (Continued)

- Add tracking blocking extensions to all your browsers
  - Ghostery, Adblock Plus, DuckDuckGo, uBlock Origin, Privacy Badger, etc.
  - Turn off most “Location Services” on your phone and tablet
    - Or, at a minimum, set their use to “Only when using App”
- Change Email setting to view mail as “Text Only”
- Cookies: Take the time to select cookies you want/don’t want on web sites

Is There Any Way to Prevent Targeting? (Part 3)

Level 2

- Do all of Level 1, then:
- Look before you leap
  - Connect only with trusted online resources and research sites before you use them
  - Lurk before you leap into blogs, social media networks, online forums, etc.

Is There Any Way to Prevent Targeting? (Part 4)

Level 2 (continued)

- Don't do research related to your work:
  - At sites that could trace the visit back to you
  - With your employer's email address
  - From a personal account on your office computer
- Turn on firewalls and use the strongest settings your browser allows HTTPS://
- Delete browser history and cookies regularly
- Use Private browsing

Is There Any Way to Prevent Targeting? (Part 5)

Level 3

- Do all of Level 2, then:
- Set up and use a VPN
- Use the Tor browser
- Use different email accounts for different purposes
- Limit what you share about yourself on social media
- Opt out of any data collection and don't participate in surveys that ask for personal information

Security

- Security is about preventing illicit access to your assets, online resources (email, social media sites, etc.) and your home and work networks
  - **Level 0**
    - Buy identity theft insurance
  - **Levels 1, 2, and 3**
    - Take steps to prevent others from gaining access to your financial accounts, email accounts, and social media pages

Passwords – Not Much Security

But it's all we have now

- Passwords are primary means of access to online resources
  - What's more secure
    - #$%10
    - John……Smith
  - Different passwords for different accounts
    - Most secure
      - Email
      - Bank
      - Work network login
    - Next secure
      - Amazon, other online retailers
    - Least secure – Social media, others that have little value to an intruder

Authenticating Access Rights

Protecting resources by restricting access to them

- Three methods of authenticating access rights
  - Something you know (User ID/Passphrase combination)
  - Something you have (token or one-time code)
  - Something you are (biometrics – retinal scan, fingerprint)
- Requiring all three is most secure
- Requiring two provides reasonable level of security
  - Called “two-factor authentication”
- Use of only one method least desirable
  - Yes, even fingerprints can be “hacked”

Where Possible, Use Two-Factor Authentication

- Email
  - Google and others
    - Require UID/Passcode pairs (something you know)
    - Permit use of one-time code sent to another device (something you have)
  - Mobile devices use fingerprint readers or face recognition if available
  - Financial institutions increasingly require two-factor authentication for certain transactions
    - More on that later

Using Cloud Storage

(iCloud, Dropbox, Google Drive, One Drive, etc.)

- Cloud storage is only as secure as:
  - The strength of your access limitations
    - Understand the process the provider is using and its security
    - Take advantage of and enable any security features the provider may have
    - Use strong passphrase that you don't use anywhere else
- To protect the security of the files you store in the cloud
    - Consider using different providers to store different categories of files (security through obscurity)
    - Use (free) encryption for important files (i.e., VeraCrypt)

Email and Financial Transaction Security (Part 1)

- Email dos and don’ts
  - Do use two factor authentication where available
  - Do turn off html and view mail in text only
    - Remember web bugs? Readnotify.com
  - Don’t check your mail using Starbuck’s network
  - Don’t open mail from unknown or untrusted sources – delete

Email and Financial Transaction Security (Part 2)

- Email dos and don’ts
  - Don’t respond to any message that requests personal information, even if it purports to be from your bank
  - Have multiple mail accounts and use one only for providing an mail address to sites that require it for access
    - Yopmail

Online Banking and Investment Management

- Take steps to limit your own authority to send wires and conduct online transactions
- Use two factor authentication when available
- VERY strong passwords
- Turn on daily account updates from your bank
- Turn on email notifications for credit card transactions exceeding a defined amount

Choice of Networks and Network Security

- Your computers, phones, and tablets
  - Work or home networks can be trusted
  - Carrier data networks generally secure and trustworthy
  - Turn OFF automatic connection to unknown WiFi hotspots
  - Consider using VPNs when traveling
    - Reduces, but does not eliminate dangers of open networks
  - Free or other public networks should not be trusted for anything other than reading the paper, doing a Google search, getting directions

Secure Communications to/from Your Mobile Device

- Use VPNs on mobile devices
- Use Signal or WhatsApp (IOS and Android) for Phone calls and text messages
  - End to end encryption of IM and phone calls over Wifi network to anyone in address book who also uses app

Your Obligation to Protect Company Assets

- Limit your work and business communications to your company issued computers, phones, tablets, etc.
- Follow all security protocols on those devices
- Do not use your own phone or laptop for any business purposes

Unless…

BYOD Considerations
(**B**ring **Y**our **O**wn **D**evice – Part 1)

- BYOD is using your personal cell phone, tablet, and/or laptop for business purposes
  - Saves employer cost of supplying devices to employees
  - Relieves employee of carrying two phones, tablets, laptops
  - Allows employee choice of devices/operating systems for work

BYOD Considerations
(**B**ring **Y**our **O**wn **D**evice – Part 2)

- Three different configurations
  - Employer approval with set of requirements and guidelines
  - Employer permits use of personal devices alongside of company-provided devices
  - Employee uses personal devices without formal permission or guidelines

Potential Issues With BYOD
(**B**ring **Y**our **O**wn **D**evice Part 3)

- Implementing a workable BYOD system is all about managing expectations
  - Employer expectations
  - Security staff expectations
  - Employee expectations
  - Situations nobody thought about

Guide to Successful BYOD Use

(**B**ring **Y**our **O**wn **D**evice – Part 4)

- The Employee
  - Find, read, and follow all employer policies regarding BYOD use and permitted company access to your device
  - If there is no BYOD policy, step up your own security practices on your devices (to “Level 3”)
  - Understand what may happen if your device is breached and gives unauthorized access to the company network
    - Your access will be shut off
    - Company may want to wipe your device to protect its network

Guide to Successful BYOD Use
(**B**ring **Y**our **O**wn **D**evice – Part 5)

- The Employee
  - Remember that in litigation and some other matters you have an obligation to produce all company data in your possession and maybe personal data if it is mixed with work files
    - Keep work files separate from your personal files
    - Use only company email for work and personal email for personal messages

A Few Words on Mobile Device Settings

- Both Apple and Android phones and tables have settings that can improve or degrade privacy and security on the device
- You should take the time to understand what each of those settings does (and does not do) and then decide whether to allow or restrict its use
- The separate resource listing points you to some articles that show how to access and change the settings for both Apple and Android phones and tablets. Please use them.
- Or, search for “phone privacy settings” to find the best resource for you

DISCLAIMER

Disclaimer: This information is not legal advice and cannot be relied upon as such. Any suggested changes in wording of contract clauses, and any other information provided herein is for general educational purposes to assist in identifying potential issues concerning the insurability of certain identified risks that may result from the allocation of risks under the contractual agreement and to identify potential contract language that could minimize overall risk. Advice from legal counsel familiar with the laws of the state applicable to the contract should be sought for crafting final contract language. This is not intended to provide an exhaustive review of risk and insurance issues, and does not in any way affect, change or alter the coverage provided under any insurance policy.

Questions?

Re: Course Content

Tony Whitledge, J.D.
Tony@Whitledge.org

Re: Insurance Programs

Sandip R. Chandarana, J.D., Director
Professional Underwriters Agency (PUA)
2803 Butterfield Road, Suite 260
Oak Brook, IL 60523
630-861-2330
Sandip@PUAInc.com

For case notes and articles on design-build decisions and other case law, visit: www.ConstructionRisk.com.