

NOAC 2024

CU Boulder



# Information Security Consideration for Lodges

Vincent Cosomano • Frank Davis • Paul Lanzi

# Meet Your Trainers

- Yerba Buena Lodge
- Eureka, CA  
(now: San Francisco, CA)
- Vigil Name:  
Rapid Talking Flying Squirrel

We love  
information  
security 😊



Paul Lanzi



# Meet Your Trainers

- Kintecoying Lodge
- Staten Island, NY  
(now: Rockville, MD)
- Vigil Name:  
Deep Thinker
- Replace picture with your  
headshot. (Right click →  
Replace image)

We love  
information  
security 😊



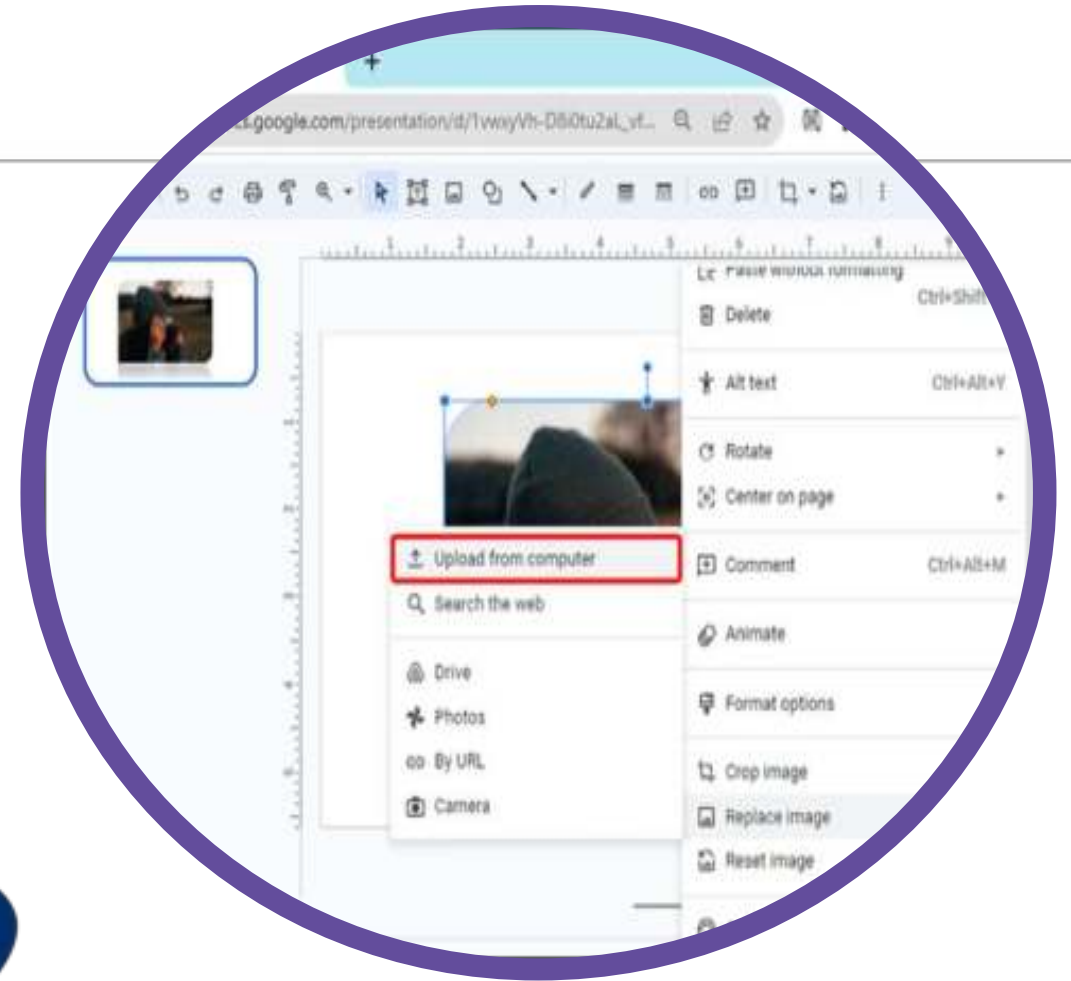
Frank Davis



# Meet Your Trainers

- O-Shot-Caw Lodge
- Miami FL
- Vigil Name: Grasshopper

We love  
information  
security 😊



Vincent



# Learning Objectives

1. What is CIA?
2. Why care about Information Security and PII?
3. Where might PII sneak in?
4. Best and Worst Ideas
5. Mitigation and Remediation
6. Available Resources





# Agenda

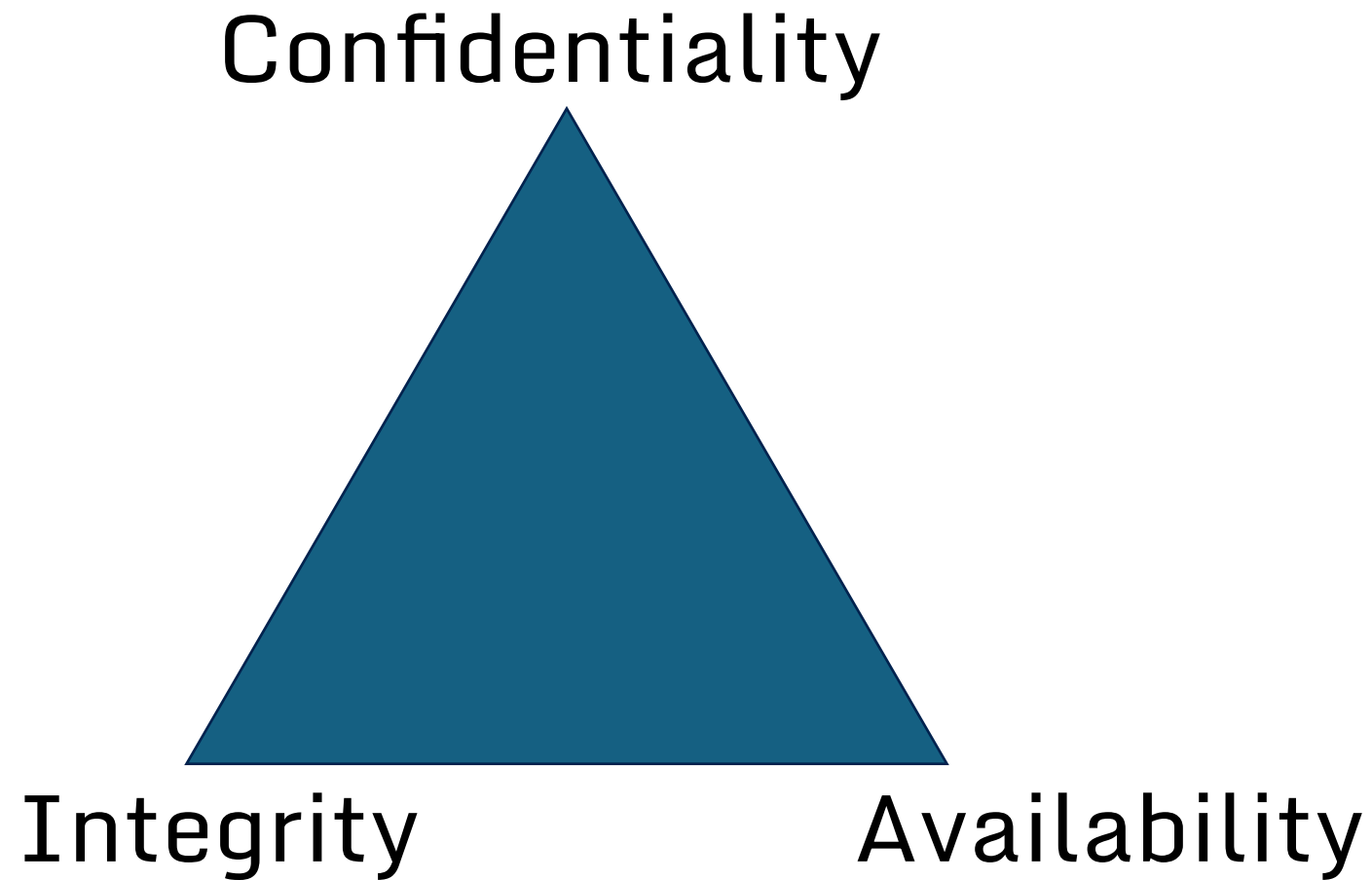


We love information  
security 😊

- What is CIA?
- Why care about Information Security and PII?
- Where might PII sneak in?
- Best and Worst Ideas
- Mitigation and Remediation
- Available Resources



# What is CIA?



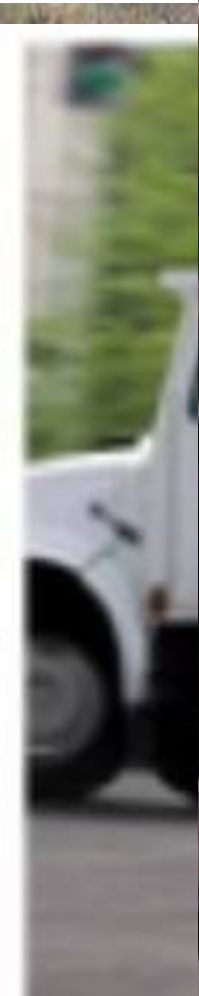
# What is PII?

- Personally Identifiable Information
  - Examples of PII:
    - Name (in combination with any of the below...)
    - Email address
    - Birth date
    - Social Security Number
  - Legal definition varies by state / there is no federal definition
- Duty to Protect
  - Part of the agreement to use BSA and OA systems including LodgeMaster is to take seriously your Duty to Protect any information you have access to in those systems





# Why care about information security?



# Why is this bad?

- Several attacks □ more information compromised □ bigger attack
- Password re-use attacks
- Ransomware attacks
- Information Disclosure Laws in some states
- Arrowmen's expectation: Protect the data that we give you



# Shared Responsibility

Data is safest  
when it stays in  
the source  
system

You take  
responsibility  
when it leaves  
the OA  
Application



OA Applications

Commercial  
Platforms (Dropbox,  
Google Drive, etc)

Pretty much anywhere  
else



# What's Worse?

Slido game: Lodge Trading Post



# What's Worse?

Slido game: Collect/Store Medical Forms





# Where might PII sneak in?

- Exports from Lodgemaster, my.scouting or Scoutbook
  - Example: Creating a sign-in sheet for Ordeal and don't want to have to type everyone's name...
- Google Sheets / Forms for signups (i.e. Lodge Dinner)
- Discord or Slack conversations
- Forums - Scoutbook Forum, Facebook Groups, etc.
- **Thought Challenge: Where are you generating PII?**





# What's Worse?

Slido game: Vigil Weekend Signup Form



# Questions to ask yourself

---

- Are we storing more information than we need?
- When will this data be permanently deleted?
- Are we sharing it with the minimum number of people possible?
- Note: You just performed a risk analysis and now you can be a CISO!



# What's Worse?

Slido game: Sharing URLs on a flyer



# Phishing emails



# Distinguish your emails from Phishing emails

- Be as consistent as possible from one email to the next
- Use proper sentence and grammar conventions in the subject and body
- Add a unique signature at the end on your email
- Don't send or ask for sensitive information (passwords, PII, bank info, etc.)
- Spell your own name correctly
- Avoid short URLs + be careful with links to non-scouting websites
- Virus Scan your attachments before attaching them in an email



# Detecting Phishing emails

- Consistency: Is this the same person that emailed you last time?
- Is it weird? **Contact them** via some other (trusted) mechanism
  - Or... ask a friend if they think the email looks weird
- Check for misspellings, capitalization errors, grammar, run-on sentences, etc. in the subject line and body of the email.
- Hover over any links in the email, but DO NOT click on them. See if the links look from a legitimate site (including warning banners)





# Detecting Phishing emails

- Don't trust the "From:" line – it can be faked
- Does the message convey urgency? Be extra cautious
- No one will ever ask for your login password
- Non-personalized greeting
- Weird attachments or links



# What's Worse?

Slido game: Google Drive Sharing

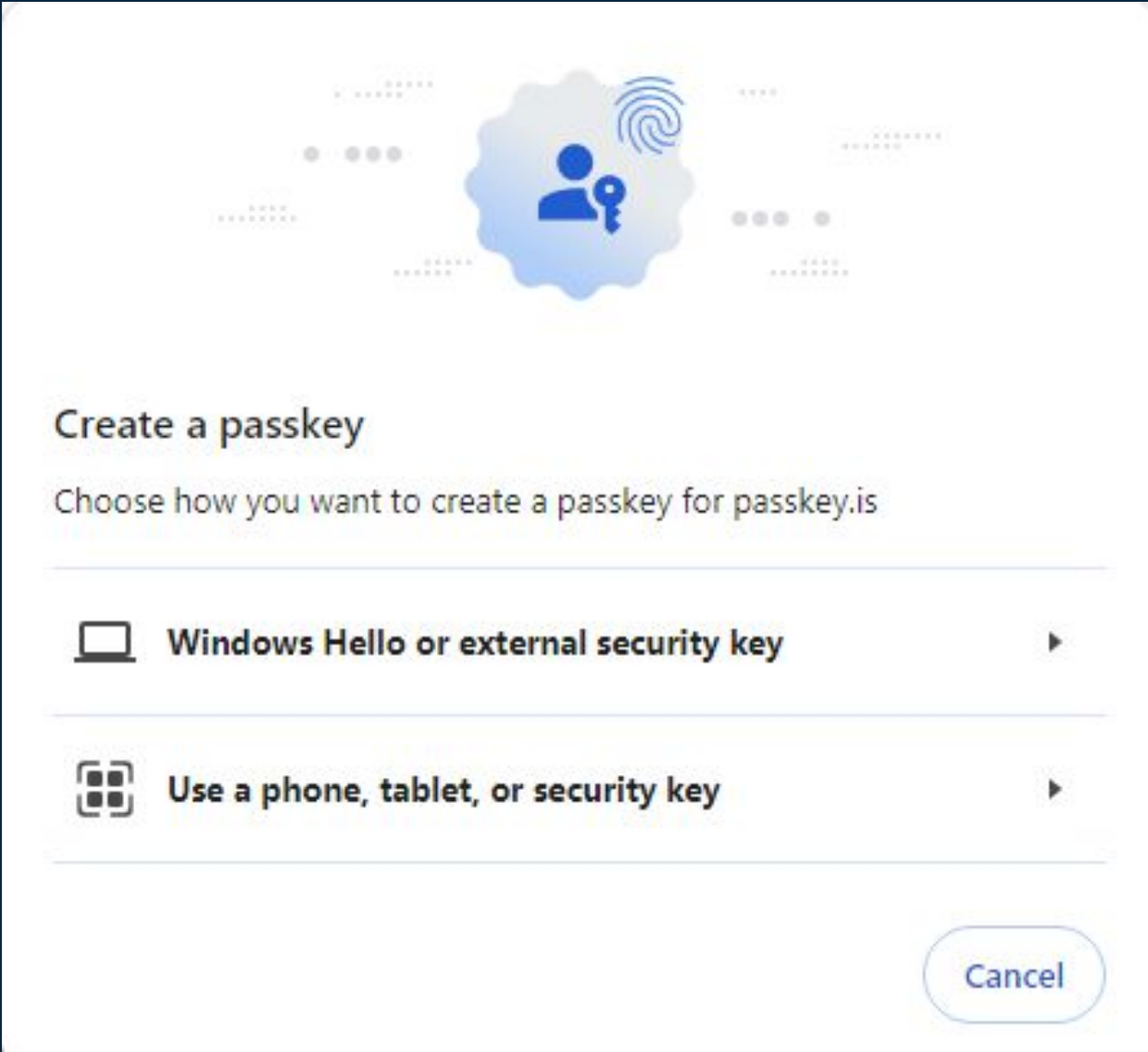


# BONUS:

## What is a Passkey?

Tired of usernames and password?

You might need a passkey!



The image shows a user interface for creating a passkey. At the top, there is a blue circular icon with a white keyhole and a fingerprint symbol. Below this, the text "Create a passkey" is displayed. Underneath, it says "Choose how you want to create a passkey for passkey.is". There are two options listed: "Windows Hello or external security key" and "Use a phone, tablet, or security key". Each option has a right-pointing arrow. At the bottom right, there is a "Cancel" button.

Create a passkey

Choose how you want to create a passkey for passkey.is

- Windows Hello or external security key
- Use a phone, tablet, or security key

Cancel



# Takeaways

- #1 - Information Security is everyone's job
  - Your IT person / tech geek can't solve this by themselves
- #2 - PII is sneaky... it gets into a lot of places
- #3 - This isn't a problem that requires money to solve. There are good, free tools out there that, when used appropriately, can keep your information secure.
- #4 - Minimize: Minimize data (you gather), minimize features (you turn on), minimize who (you share with) → this minimizes your risk.
- #5 - Go home and turn on MFA and don't re-use passwords across websites
- #5.5 - Turn on your ArrowID MFA today!



# Turn on MFA ArrowID

ARROWID   
Welcome back, Paul!

## Manage your account

Name:

Paul Lanzi [\[ Change \]](#)

Email:

@ .com [\[ Change \]](#)

Password:

[\[ Change \]](#)

Two-factor authentication:

[\[ Configure / Reset \]](#)

Want these  
slides?

URL goes here

# Appendix

