# You’re Probably Not Red Teaming

## …and Often, I’m Not Either



Deviant Ollam

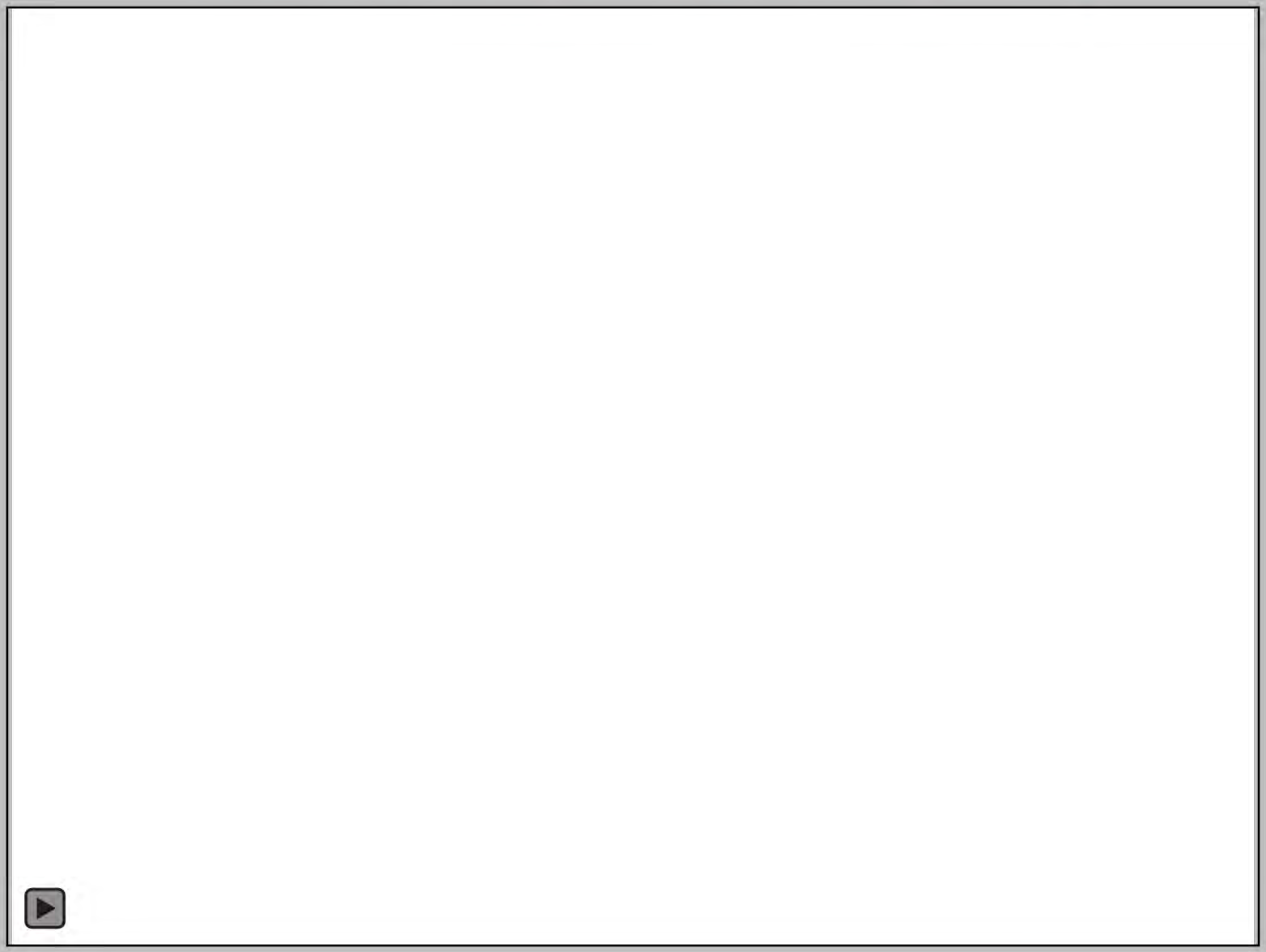
# My Job is Fun



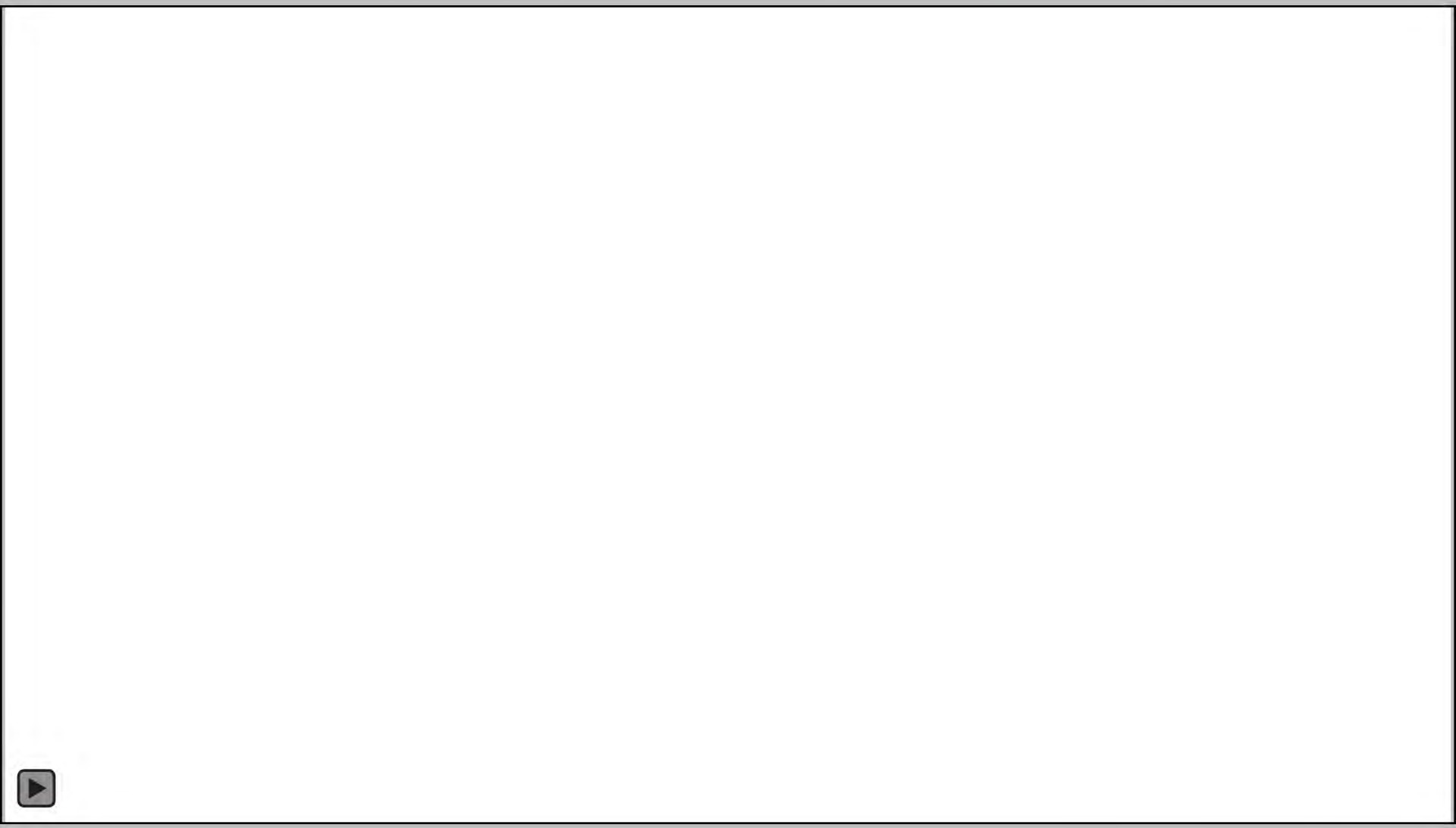
# We Don’t Belong in Here!



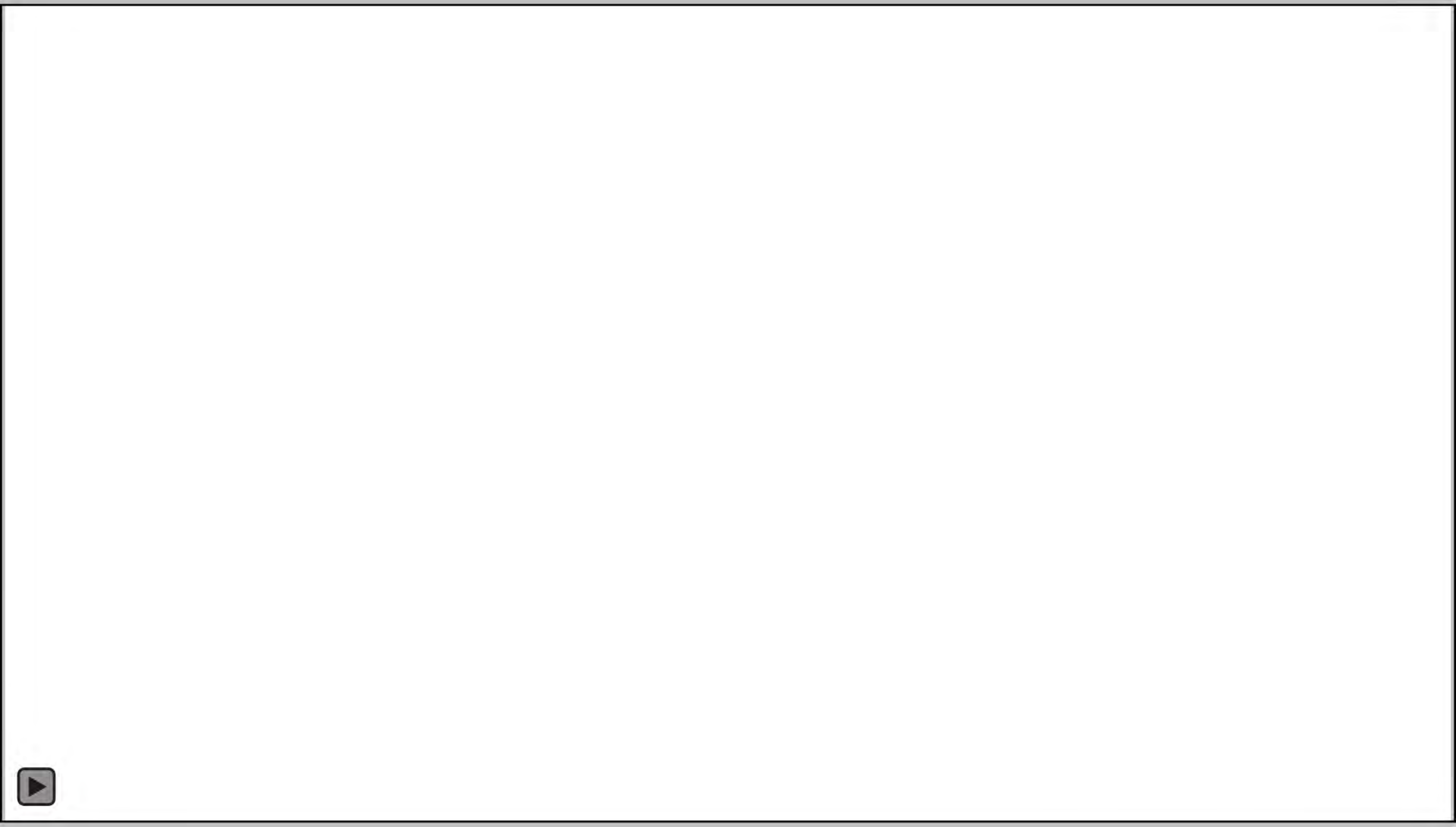
# I Get Inside Quickly and Quietly



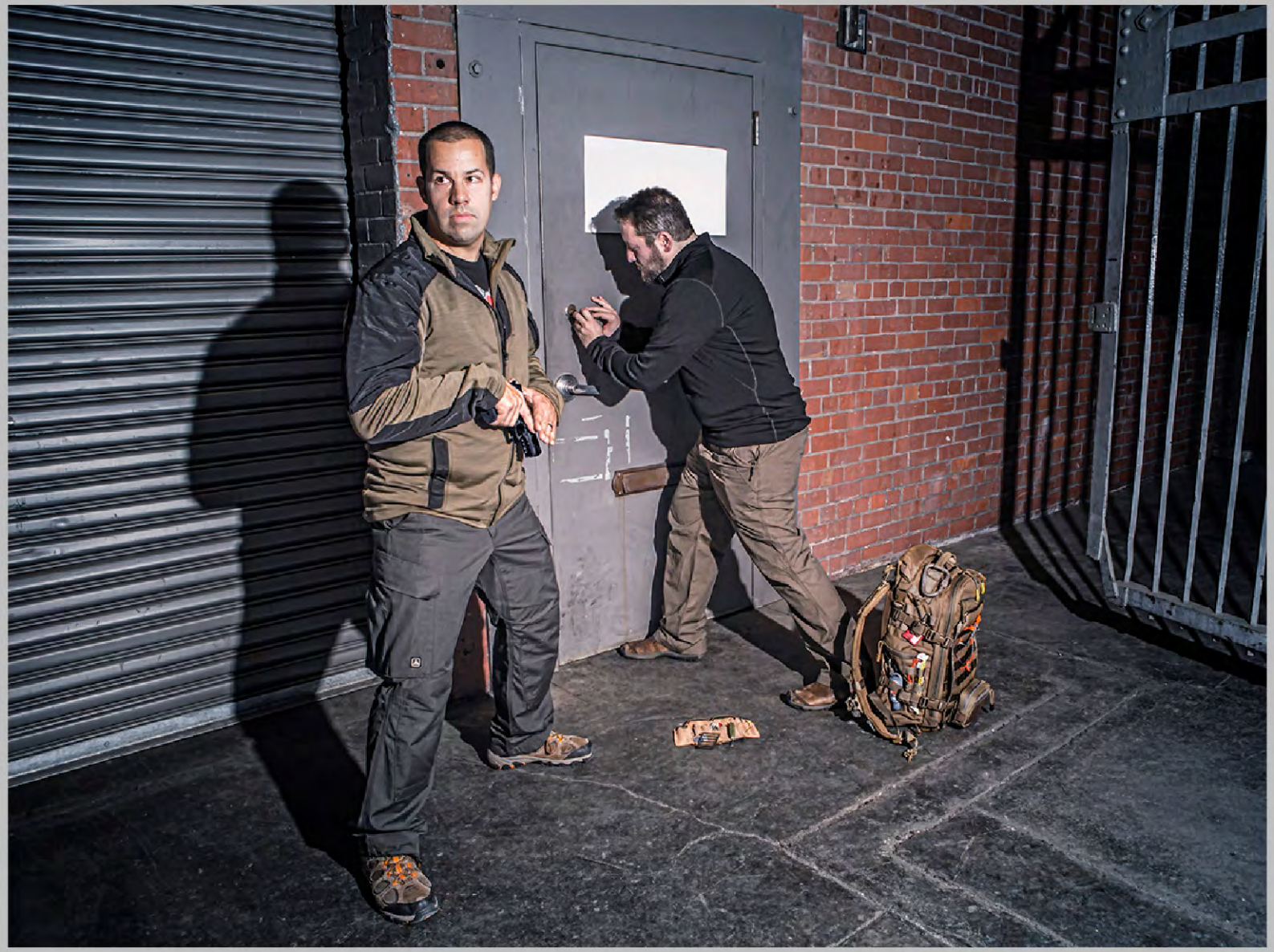
# I Get Inside Quickly and Quietly



# I Get Inside Quickly and Quietly



# People Want to Do This



# I Bet Many People Here Believe That What You Just Saw is “Red Teaming”



# I Bet Many People Here Believe That What You Just Saw is “Red Teaming”



… It’s Not.

# Where The Red Team Fits Has Been Discussed Previously... by Folk Way Smarter, Cooler, and More Attractive Than Me

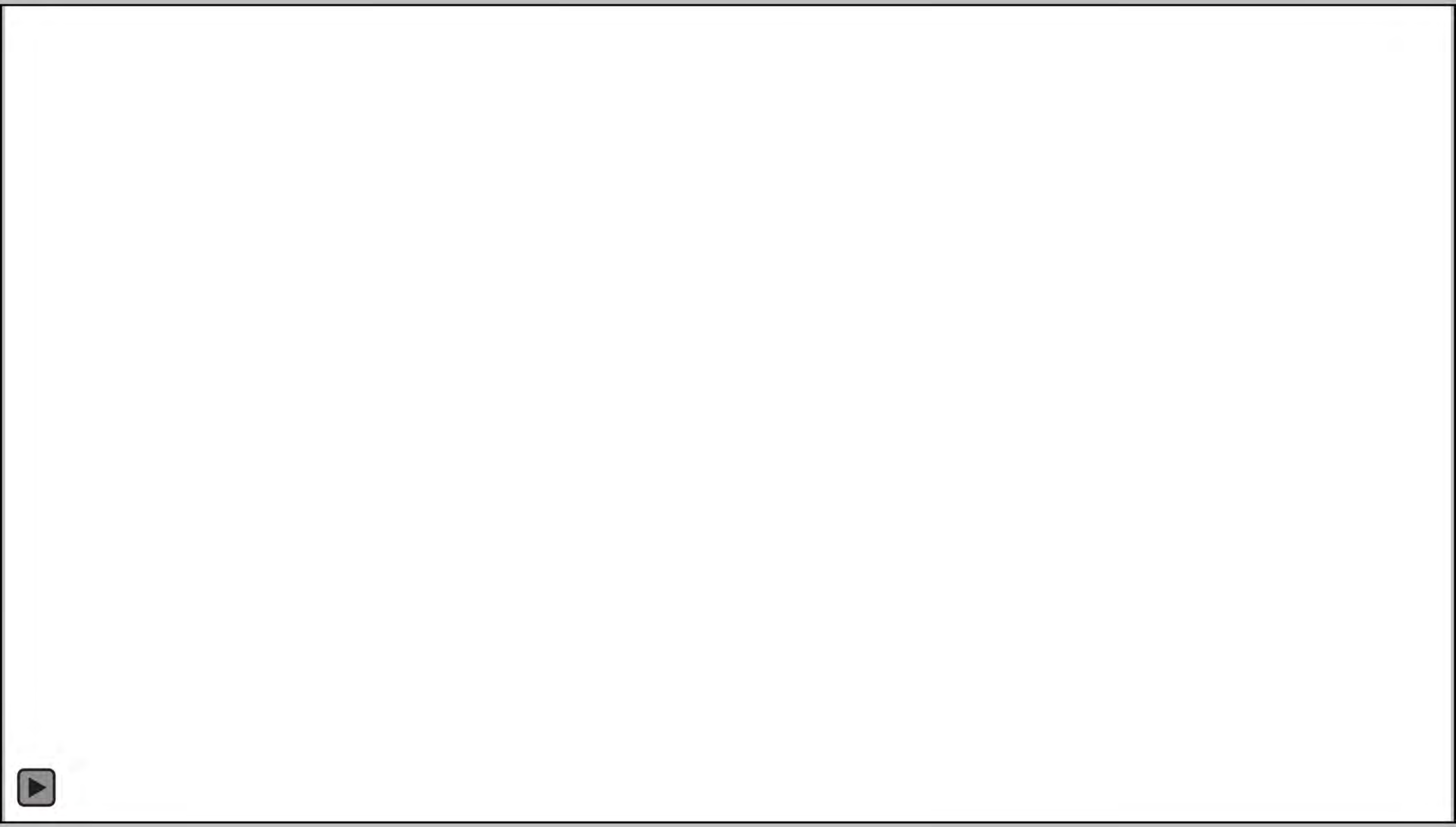









# Talk of Purple Teaming is Becoming Popular



# Talk of Purple Teaming is Becoming Popular

"That's when the Red Team sends an extra person to sit in the SOC with the Blue Team… and then they get to charge the client double."

*- Chris Gates*



# There Are Three Elements To Security



# There Are Three Elements To Security



# There Are Three Elements To Security



# Digital



# Physical



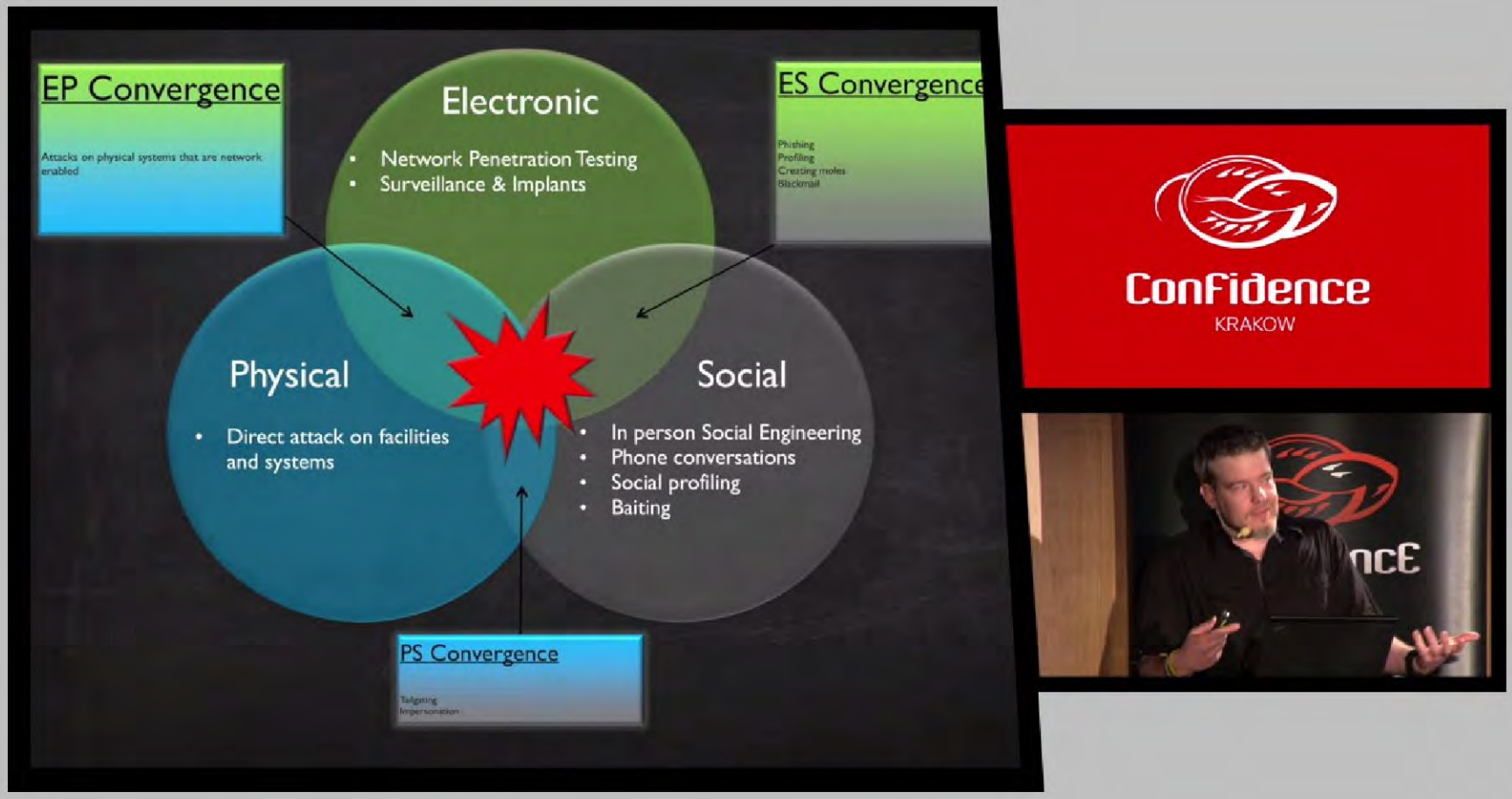
# Human



# And There's Crossover



# And There's Crossover



# Attacking via the Physical Vector



# Covert Methods of Entry



# Covert Methods of Entry



# Covert Methods of Entry



# Covert Methods of Entry



# Covert Methods of Entry



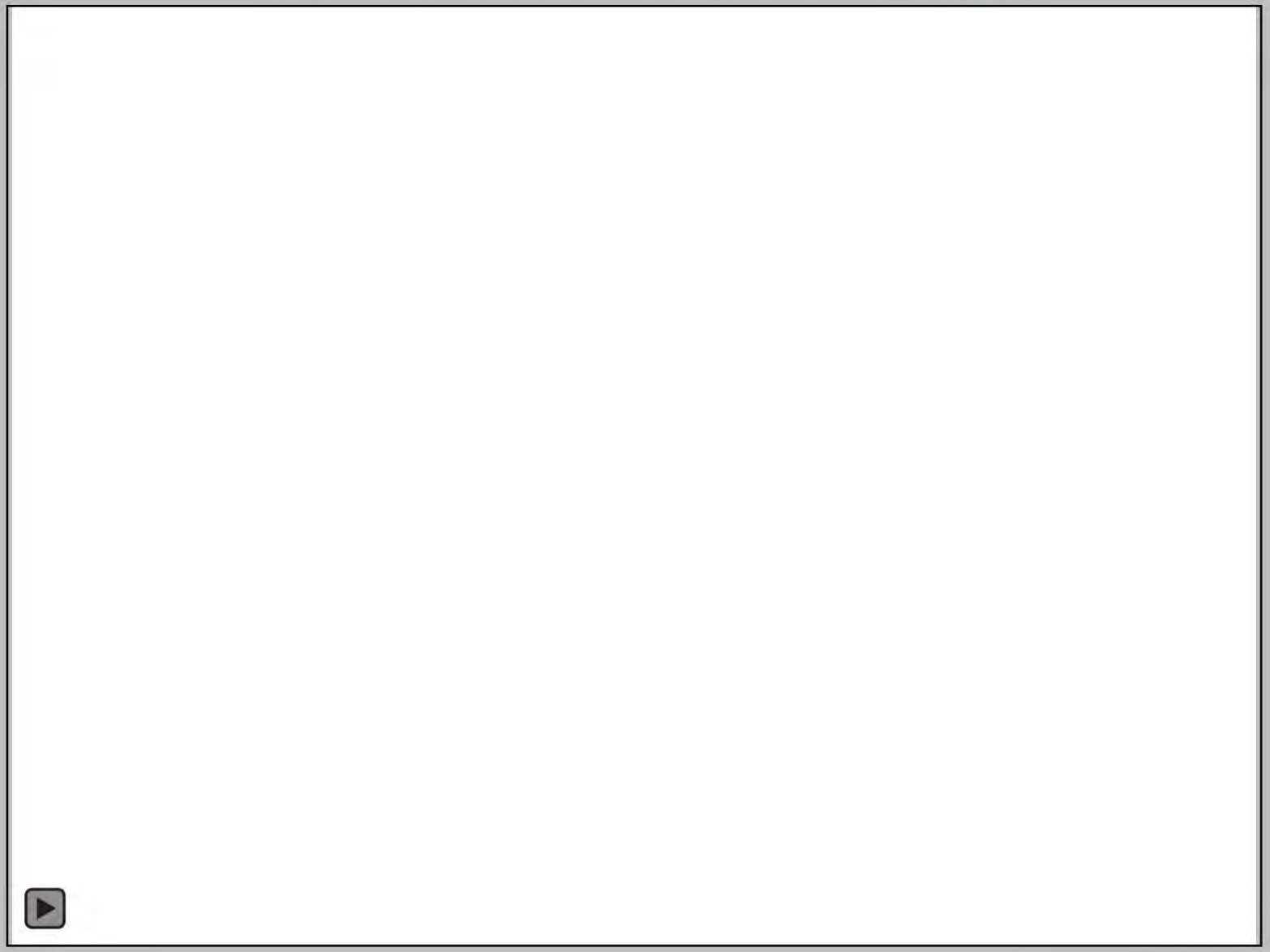
# Covert Methods of Entry



# Covert Methods of Entry



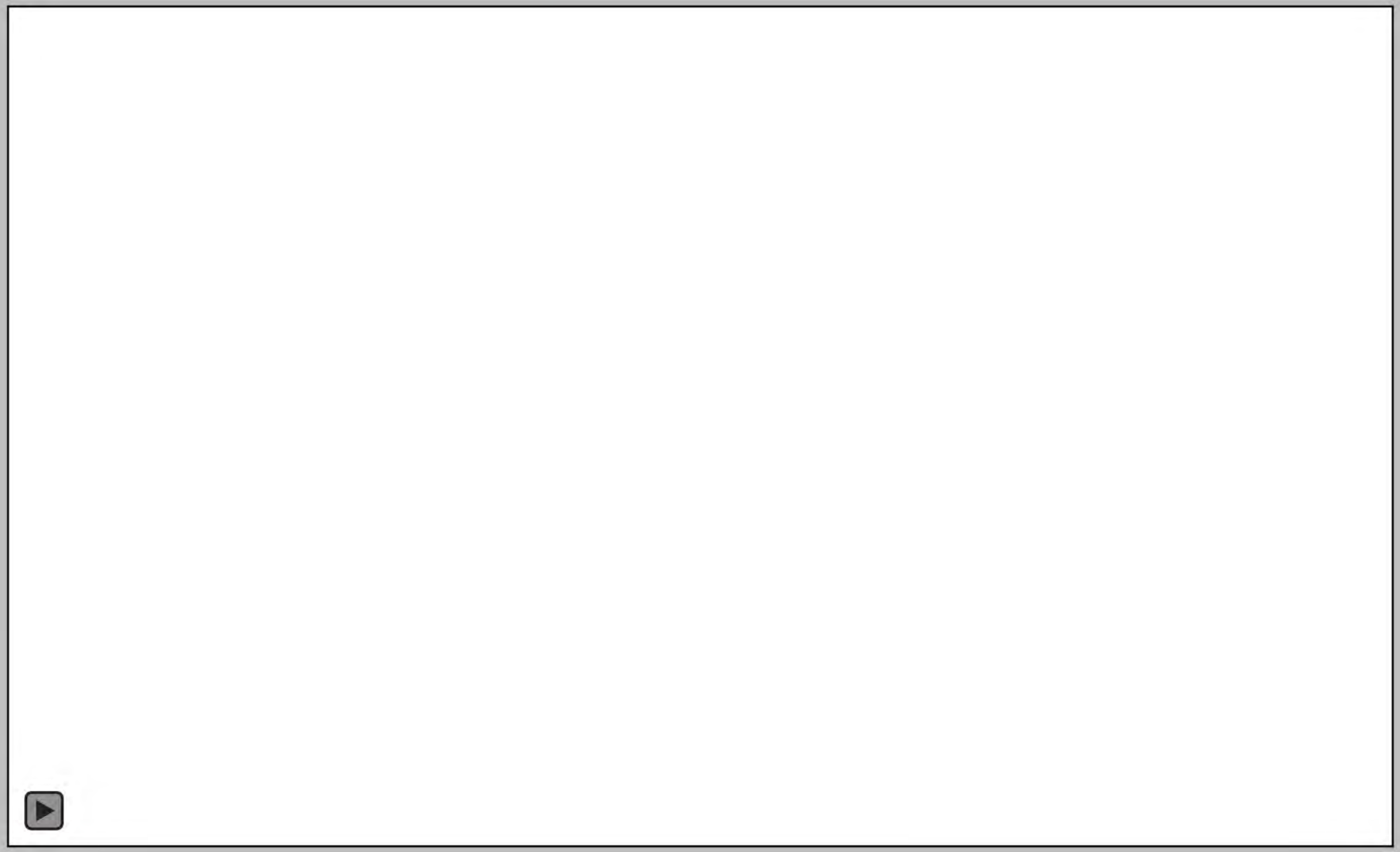
# Covert Methods of Entry



# Attacking via the Digital Vector



# Network Security & Access Control Systems



# Network Security & Access Control Systems



# Network Security & Access Control Systems



# Attacking via the Human Vector



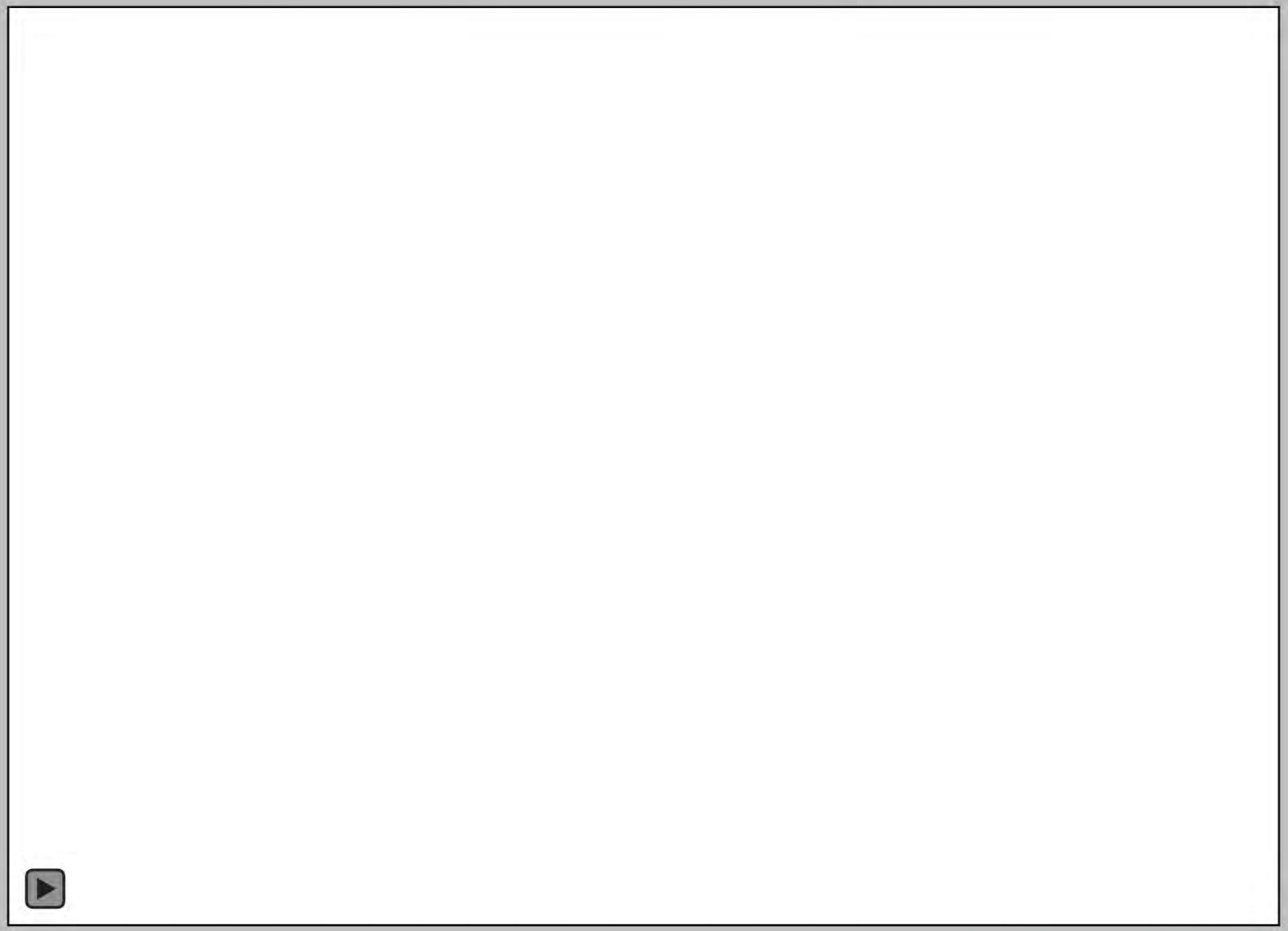
# Look Like You Belong There



# Look Like You Belong There



# Look Like You Belong There



# Look Like You Belong There



# Look Like You Belong There



# Some Stories... and Some Questions



# Story Number One: Elevator Repair



# Elevator Technician is a Great Cover Story



# Elevator Technician is a Great Cover Story



# Elevator Technician is a Great Cover Story



# Elevator Technician is a Great Cover Story



# Elevator Technician is a Great Cover Story



# A Metal Contractor Clipboard is Awesome



# A Metal Contractor Clipboard is Awesome



# So I’m in the Building…



# ...Teammate Had to Go Back to the Hotel



# I've Got Nothing But Time



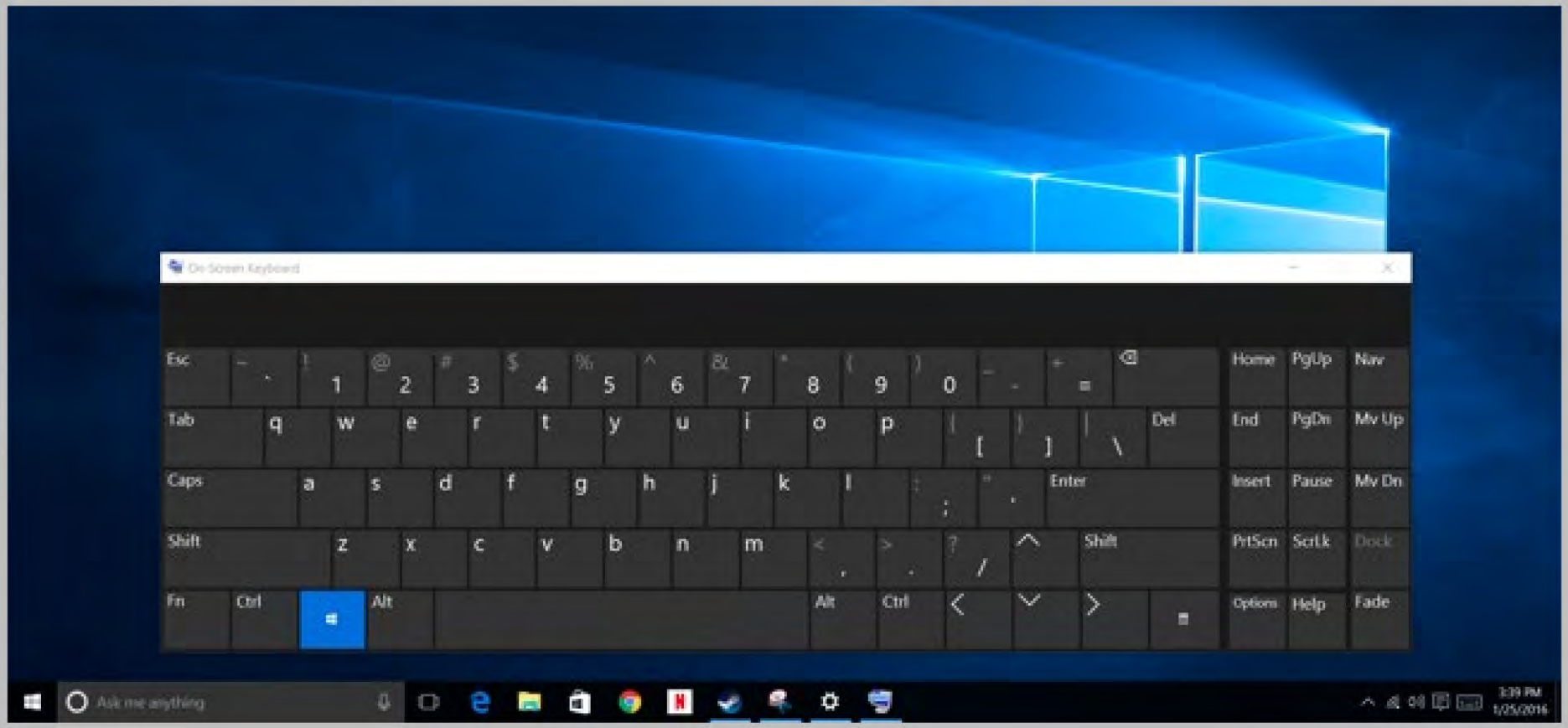
# I've Got Nothing But Time



# Things at the Hotel Were Going Slowly



# Things at the Hotel Were Going Slowly



# Then I Nearly had a Heart Attack



# I Figured it Must Be The Cleaners



# It Wasn't



# It Wasn't


OUT
OF
ORDER
1 - LOWER LEVEL
2 - MAIN LOBBY
FLOOR 3
OFFICE CENTER
OFFICES

# Fortunately, I'm a Friendly Elevator Technician



# “I’ll Have to Check the Elevator Controller in Here”



# Everyone Wants to Keep the Elevators Working



# Story Number Two: The Cable Technicians



# Preliminary Recon



# “Look Like You Belong There”
























# "Look Like You Belong There"





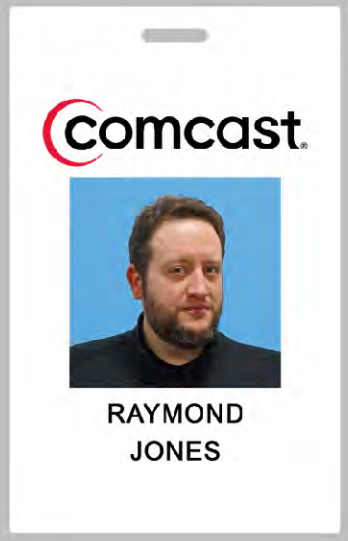
















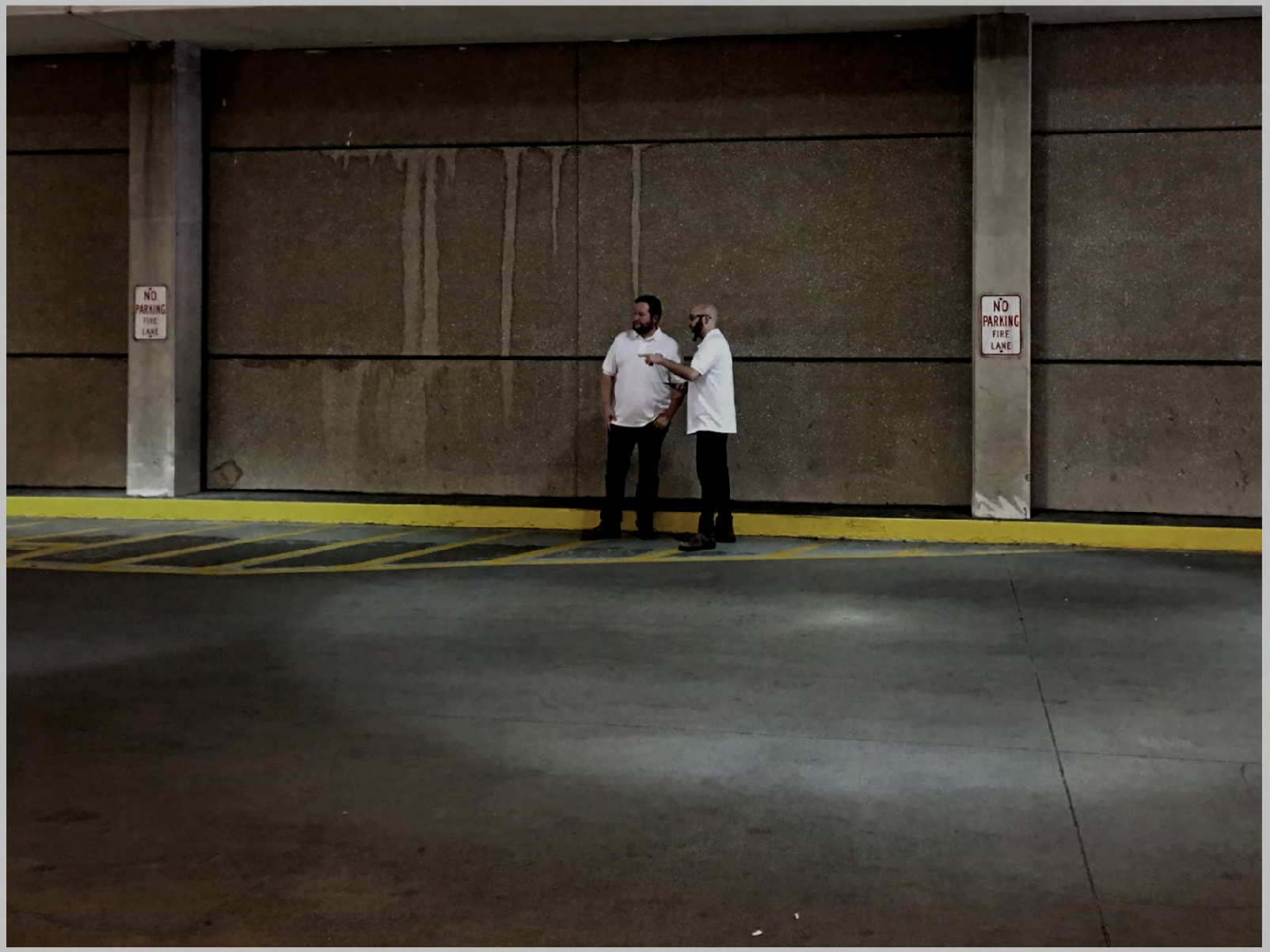
# The Cable Technicians



# The Cable Technicians



# The Cable Technicians



# The Cable Technicians



# What Would You Do?



# Make a New Friend!



# We're Totally Legit... Trust Us.



# Do You Think He Verified Our Story?



# How Did We Get In?



# How Did We Get In?



# Later, Inside the Office



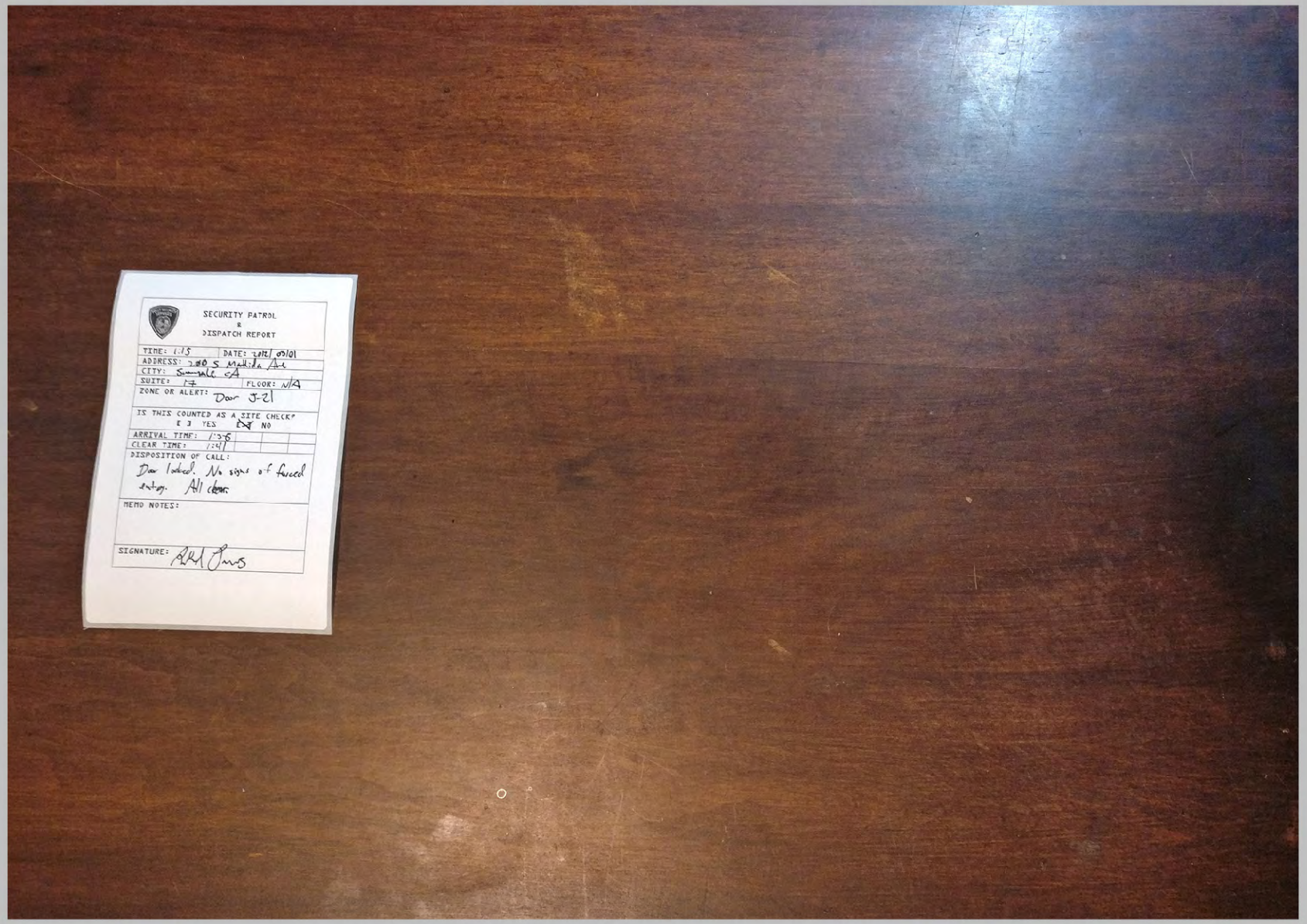
# Later, Inside the Office



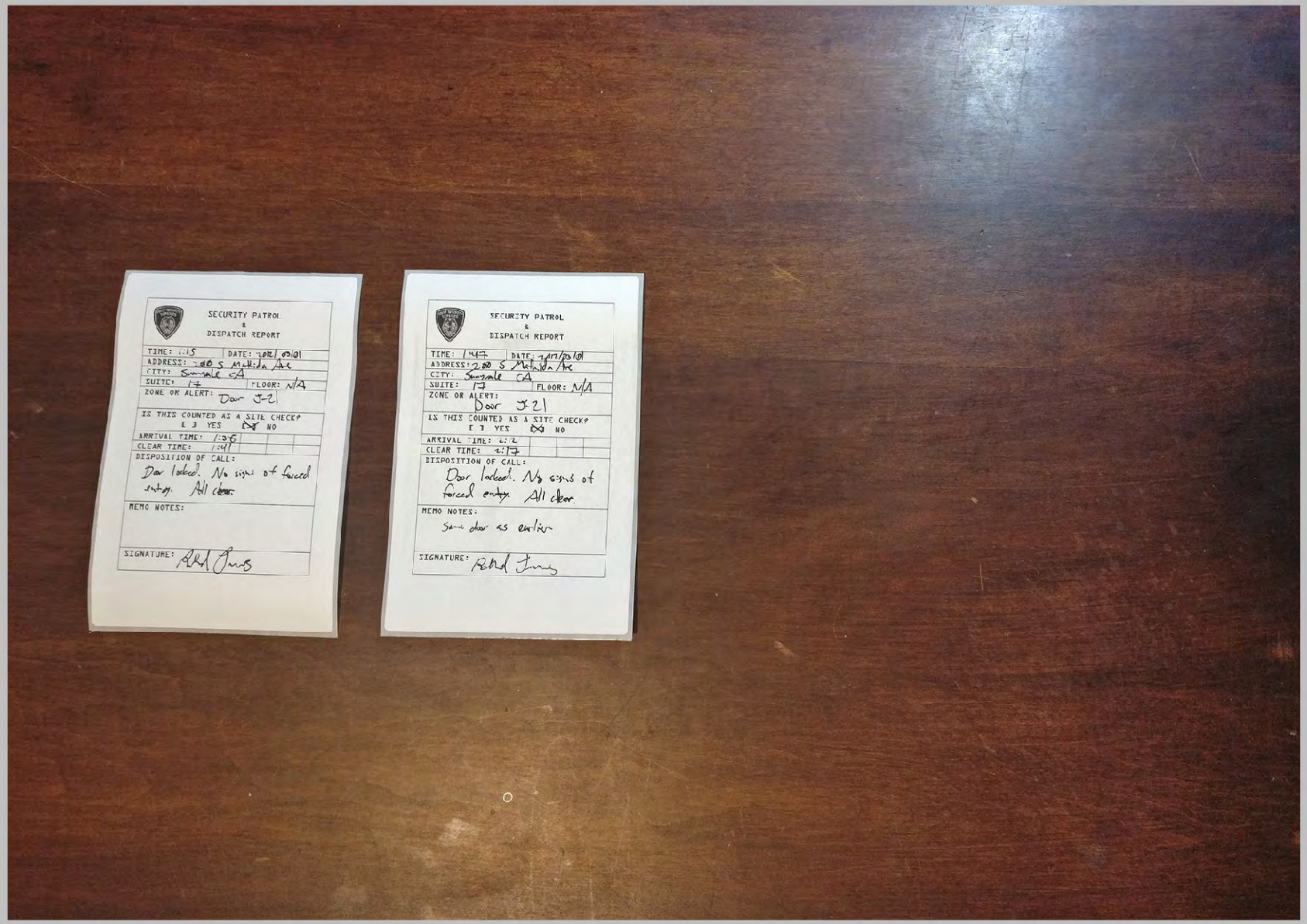
# Total Victory Winning



# The Client Actually Pulled the Dispatch Tickets



# The Client Actually Pulled the Dispatch Tickets



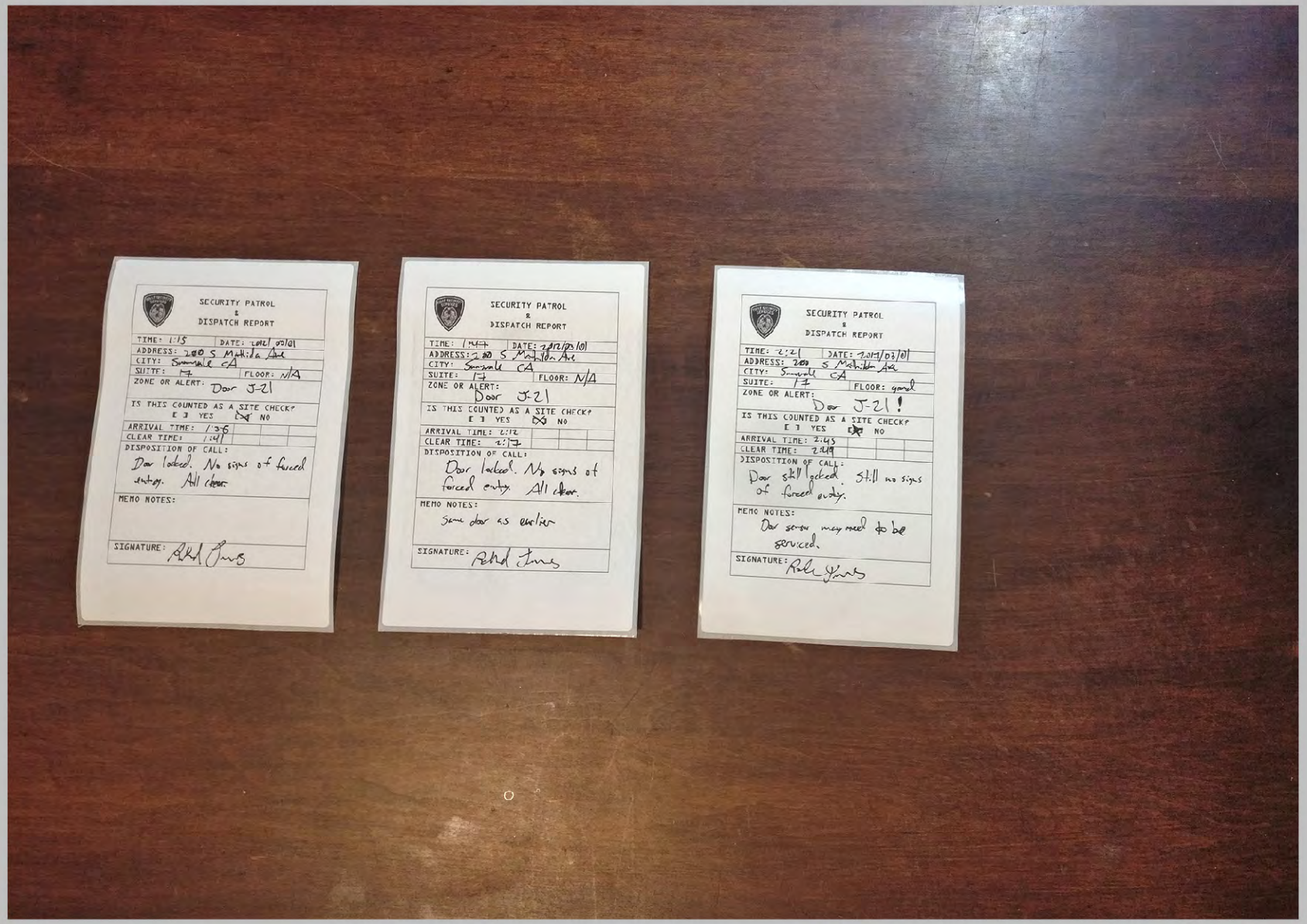
SECURITY PATROL
&
DISPATCH REPORT

TIME: 1:15 DATE: 10/2/0101
ADDRESS: 200 S Matilda Ave
CITY: Sunnyvale CA
SUITE: 17 FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK?
☐ YES ☒ NO
ARRIVAL TIME: 1:35
CLEAR TIME: 1:41
DISPOSITION OF CALL:
Door locked. No signs of forced entry. All clear.
MEMO NOTES:
SIGNATURE: Richard Jones

SECURITY PATROL
&
DISPATCH REPORT

TIME: 1:47 DATE: 10/2/0101
ADDRESS: 200 S Matilda Ave
CITY: Sunnyvale CA
SUITE: 17 FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK?
☐ YES ☒ NO
ARRIVAL TIME: 2:12
CLEAR TIME: 2:17
DISPOSITION OF CALL:
Door locked. No signs of forced entry. All clear.
MEMO NOTES:
Same door as earlier
SIGNATURE: Richard Jones

# The Client Actually Pulled the Dispatch Tickets



SECURITY PATROL & DISPATCH REPORT

TIME: 1:15 DATE: 2011 05/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 1-4 FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK? ☐ YES ☒ NO
ARRIVAL TIME: 1:36
CLEAR TIME: 1:41
DISPOSITION OF CALL: Door locked. No signs of forced entry. All clear.
MEMO NOTES:
SIGNATURE: Rob Jones

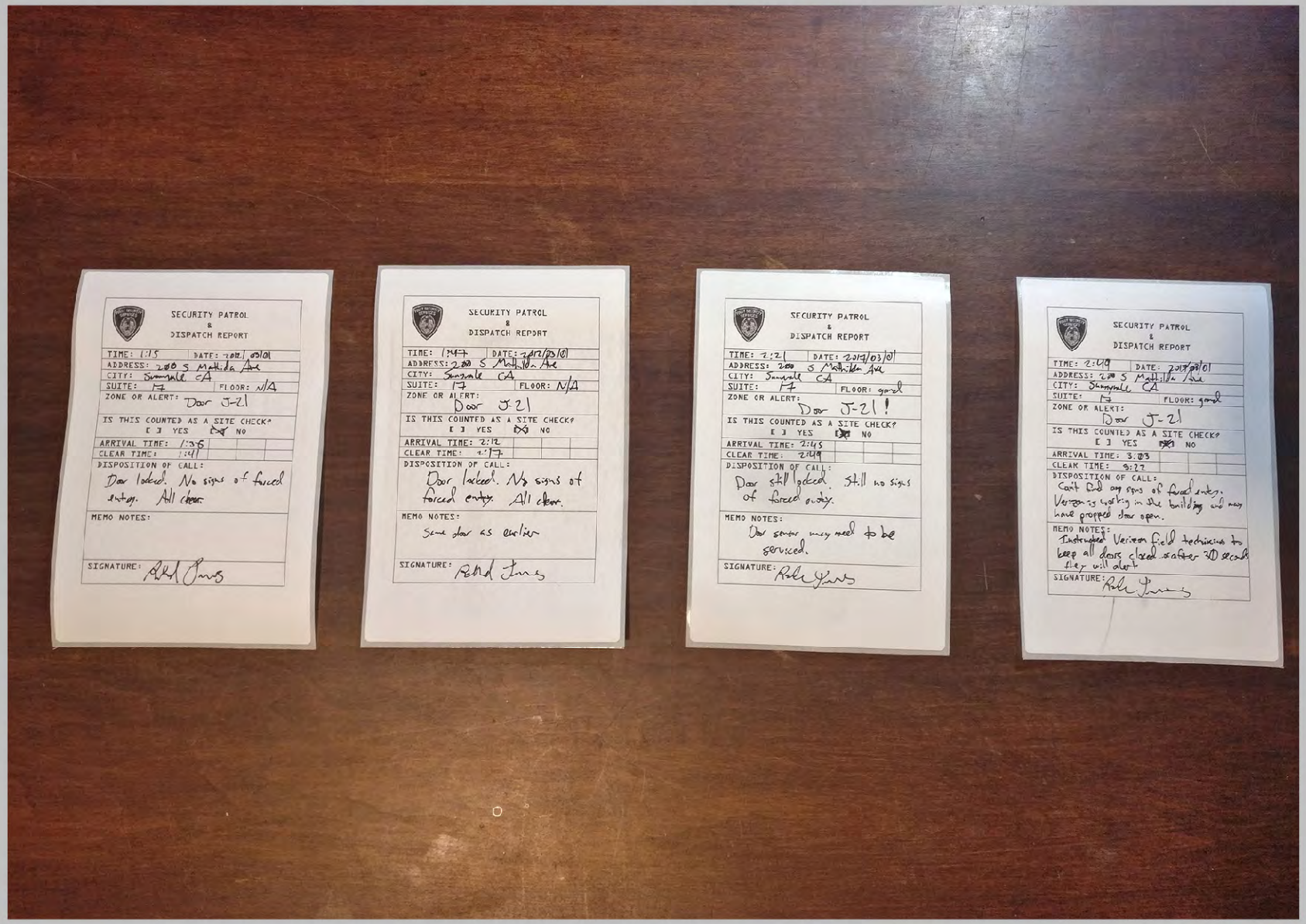
SECURITY PATROL & DISPATCH REPORT

TIME: 1447 DATE: 2012/05/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 1-4 FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK? ☐ YES ☒ NO
ARRIVAL TIME: 2:12
CLEAR TIME: 2:17
DISPOSITION OF CALL: Door locked. No signs of forced entry. All clear.
MEMO NOTES: Same door as earlier
SIGNATURE: Rob Jones

SECURITY PATROL & DISPATCH REPORT

TIME: 2:21 DATE: 2013/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 1-4 FLOOR: ground
ZONE OR ALERT: Door J-21!
IS THIS COUNTED AS A SITE CHECK? ☐ YES ☒ NO
ARRIVAL TIME: 2:43
CLEAR TIME: 2:49
DISPOSITION OF CALL: Door still locked. Still no signs of forced entry.
MEMO NOTES: Door sensor may need to be serviced.
SIGNATURE: Rob Jones

# The Client Actually Pulled the Dispatch Tickets



SECURITY PATROL & DISPATCH REPORT

TIME: 1:15 DATE: 2017/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: M FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK? [ ] YES [X] NO
ARRIVAL TIME: 1:36
CLEAR TIME: 1:41
DISPOSITION OF CALL: Door locked. No signs of forced entry. All clear.
MEMO NOTES:
SIGNATURE: Robert Jones

SECURITY PATROL & DISPATCH REPORT

TIME: 1:47 DATE: 2017/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: M FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK? [ ] YES [X] NO
ARRIVAL TIME: 2:12
CLEAR TIME: 2:17
DISPOSITION OF CALL: Door locked. No signs of forced entry. All clear.
MEMO NOTES: Same door as earlier
SIGNATURE: Robert Jones

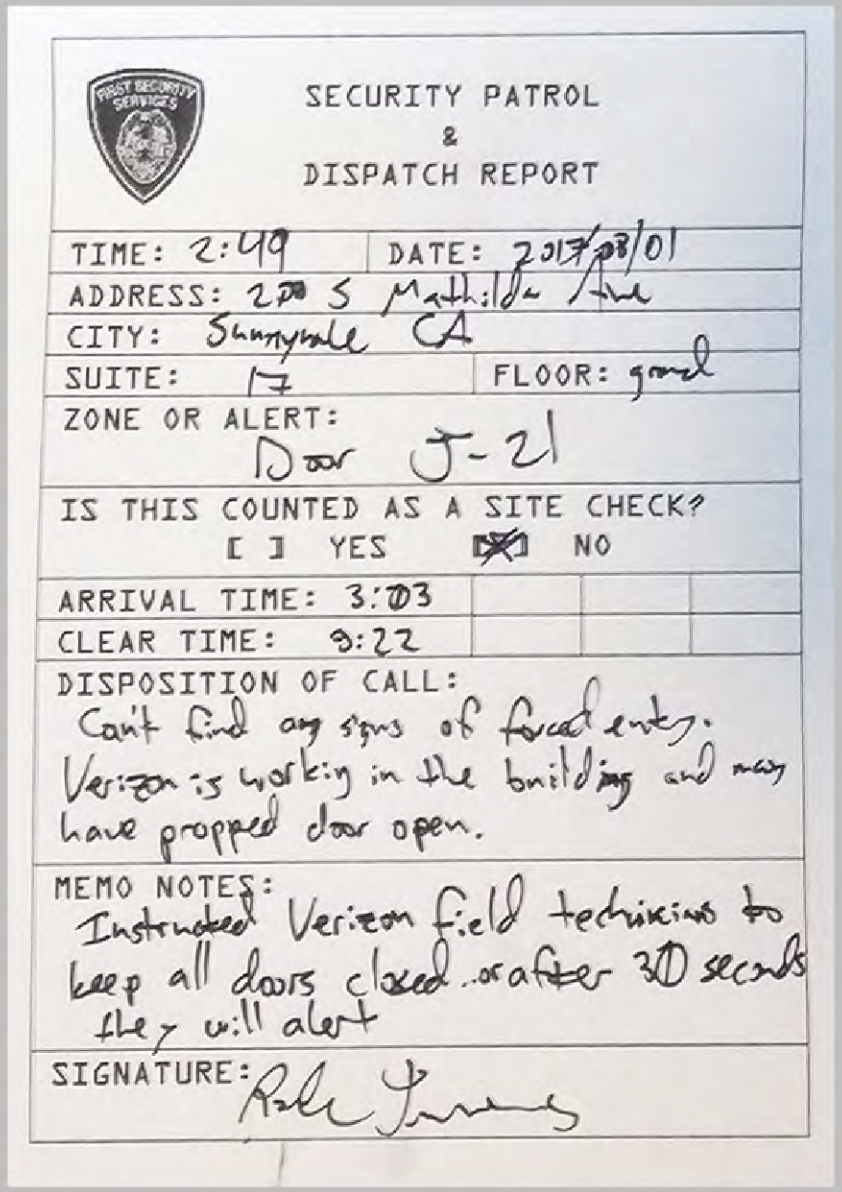
SECURITY PATROL & DISPATCH REPORT

TIME: 2:21 DATE: 2017/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: M FLOOR: ground
ZONE OR ALERT: Door J-21!
IS THIS COUNTED AS A SITE CHECK? [ ] YES [X] NO
ARRIVAL TIME: 2:45
CLEAR TIME: 2:49
DISPOSITION OF CALL: Door still locked. Still no signs of forced entry.
MEMO NOTES: Door sensor may need to be serviced.
SIGNATURE: Robert Jones

SECURITY PATROL & DISPATCH REPORT

TIME: 2:49 DATE: 2017/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: M FLOOR: ground
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK? [ ] YES [X] NO
ARRIVAL TIME: 3:03
CLEAR TIME: 3:27
DISPOSITION OF CALL: Can't find any signs of forced entry. Verizon is working in the building and may have propped door open.
MEMO NOTES: Instructed Verizon field technicians to keep all doors closed & after 20 seconds they will alert
SIGNATURE: Robert Jones

# The Client Actually Pulled the Dispatch Tickets



SECURITY PATROL
&
DISPATCH REPORT

TIME: 2:49 DATE: 2017/03/01

ADDRESS: 2[illegible]5 Mathilda Ave

CITY: Sunnyvale CA

SUITE: 17 FLOOR: ground

ZONE OR ALERT: Door J-21

IS THIS COUNTED AS A SITE CHECK?
[ ] YES [X] NO

ARRIVAL TIME: 3:03

CLEAR TIME: 3:22

DISPOSITION OF CALL:
Can't find any signs of forced entry. Verizon is working in the building and may have propped door open.

MEMO NOTES:
Instructed Verizon field technicians to keep all doors closed...or after 30 seconds they will alert

SIGNATURE: [signature]

# Who Wouldn't Trust Us?



# Story Number Three: The Armed Guards



# A Lot of the Time, Guards are Rather Untrained



# A Lot of the Time, Guards are Rather Untrained



# Armed Guards are Usually More On the Ball



# We Wanted to Grab Credentials



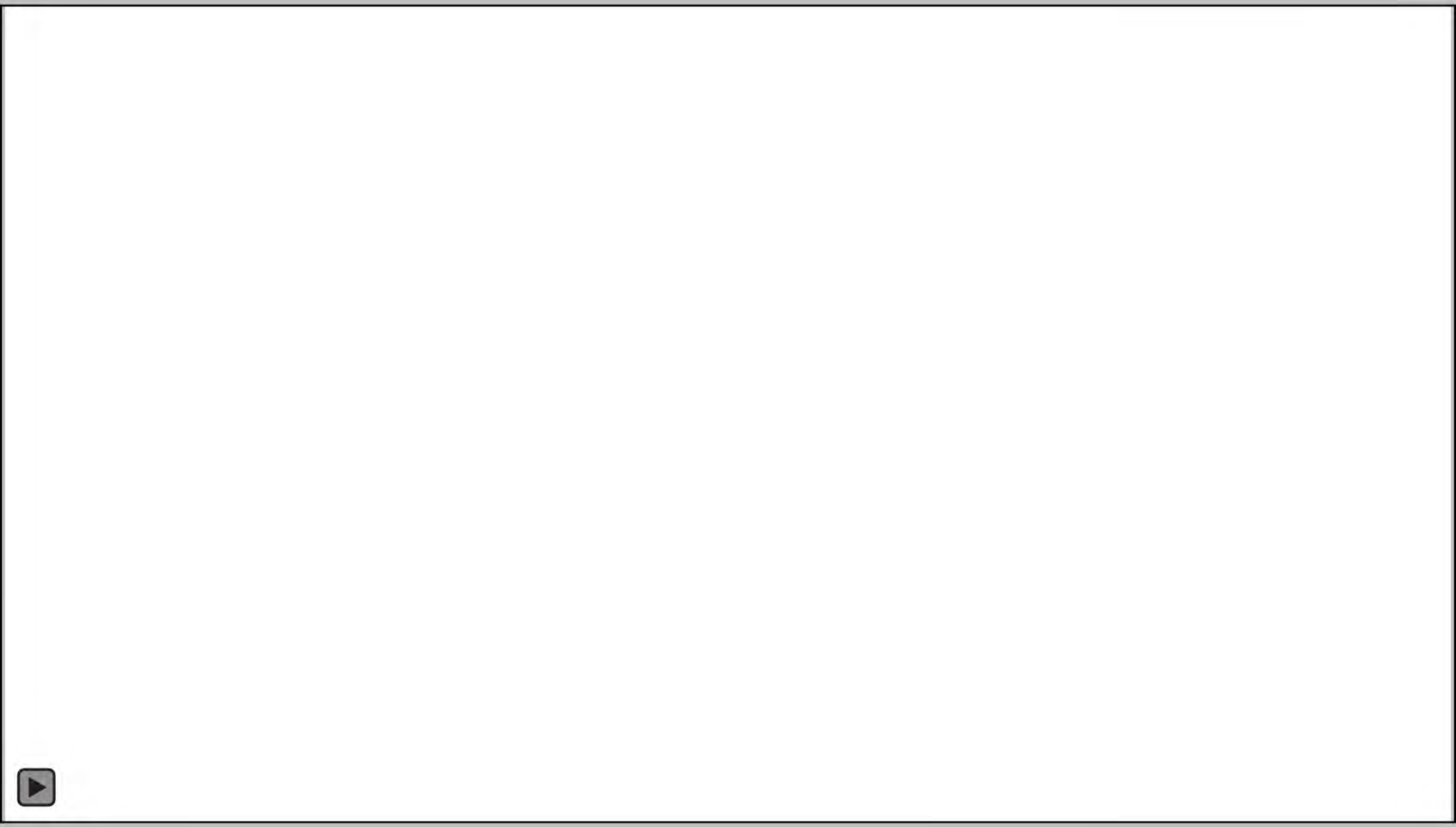
# We Wanted to Grab Credentials



# We Wanted to Grab Credentials



# We Wanted to Grab Credentials



# We Wanted to Grab Credentials



# What Do Many Armed Guards Want To Be?



# What Do Many Armed Guards Want To Be?



# Send in a Cop!



# Meanwhile, Babak is Still Out in the Car



# Rob Keeps Trying, The Guards Keep Blading



# Time to Wrap it Up and Say Goodbye



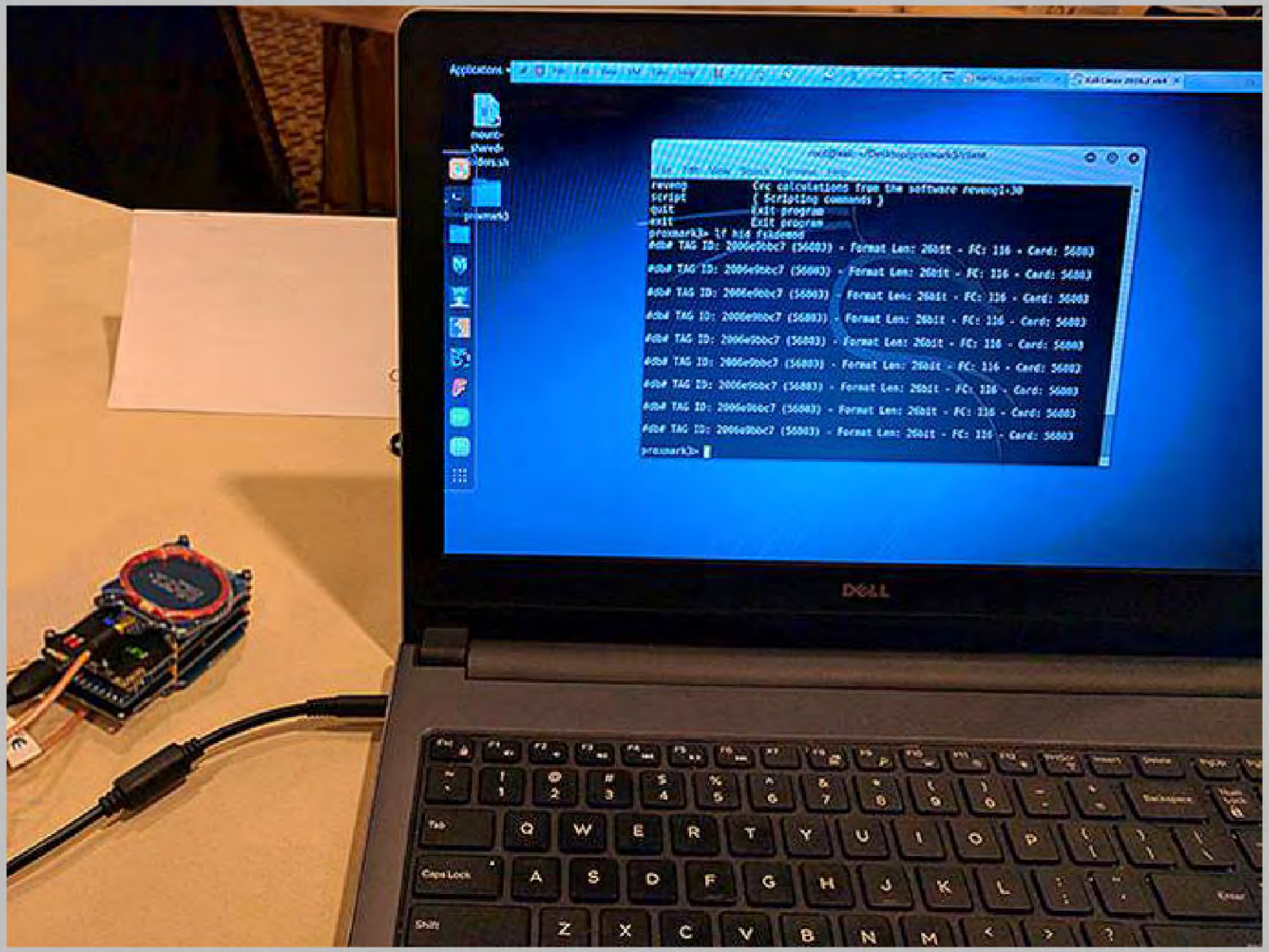
# Surprise Hug!



# Robert Comes Back to the Car



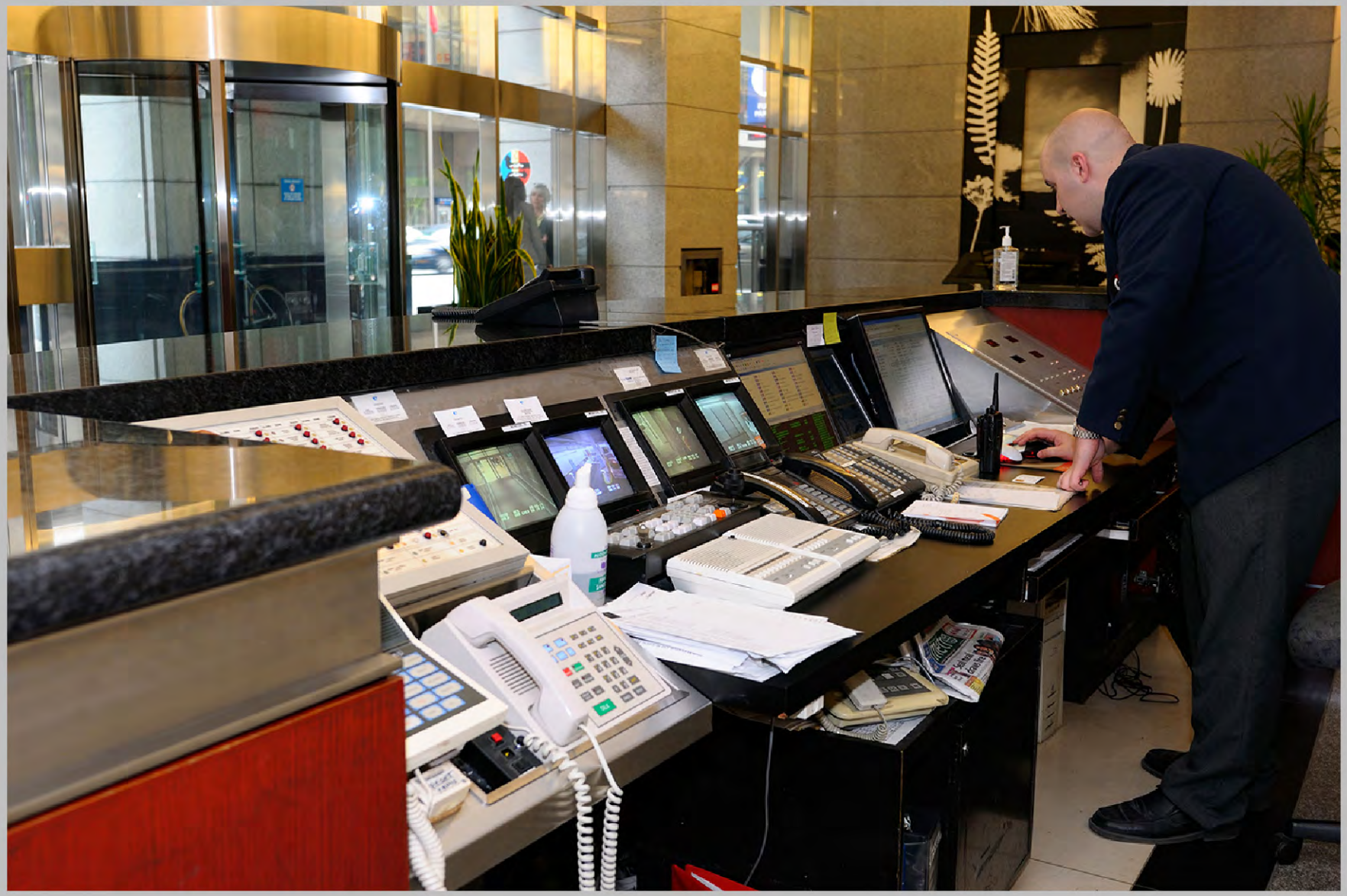
# We Checked the Logs



# Now Whose Permissions Did We Have?



# We Came Back on Their Next Shift



# We Overrode an Elevator Restriction



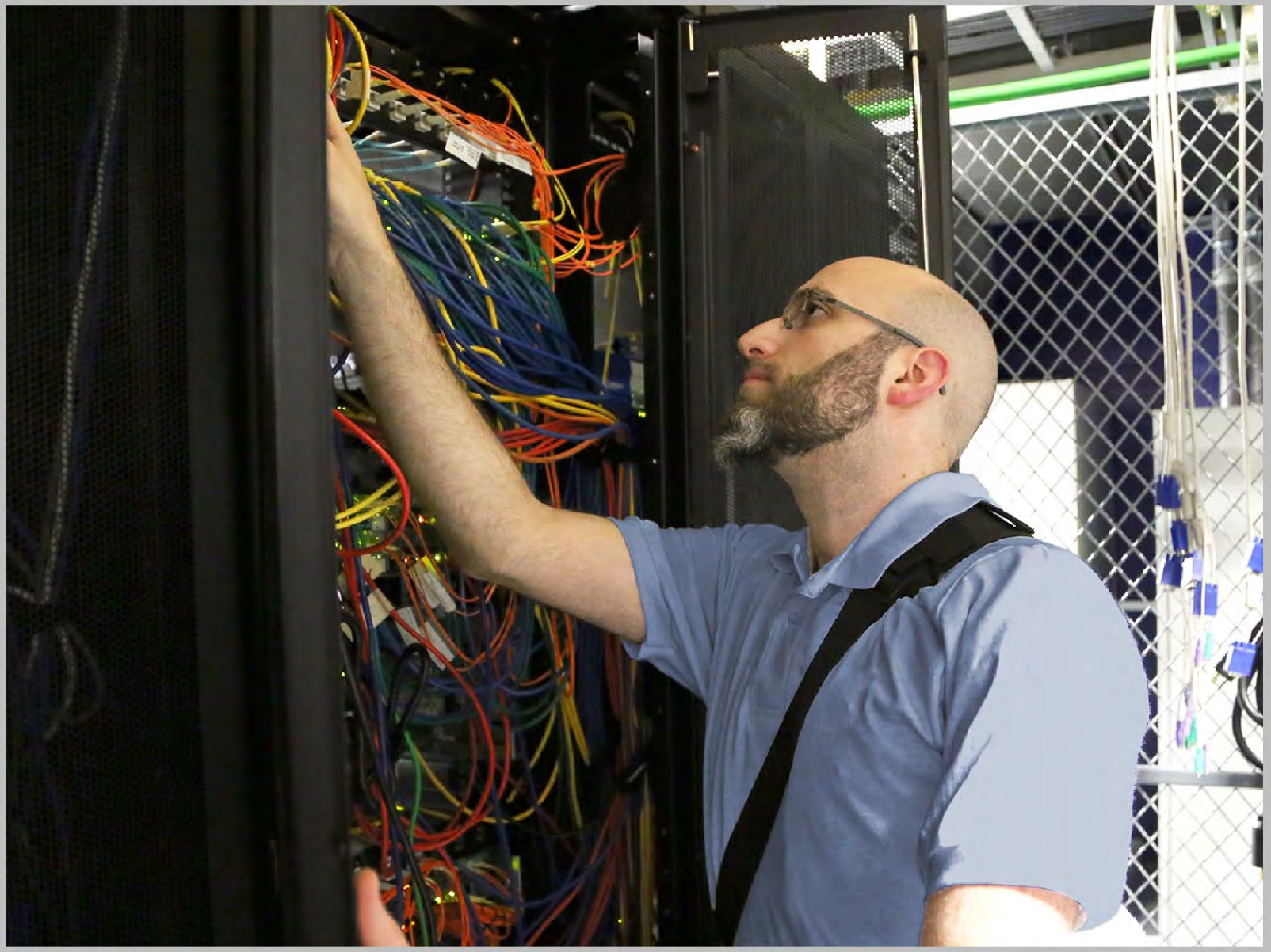
# We Picked Open a Door Lock



# We Picked Open a Door Lock



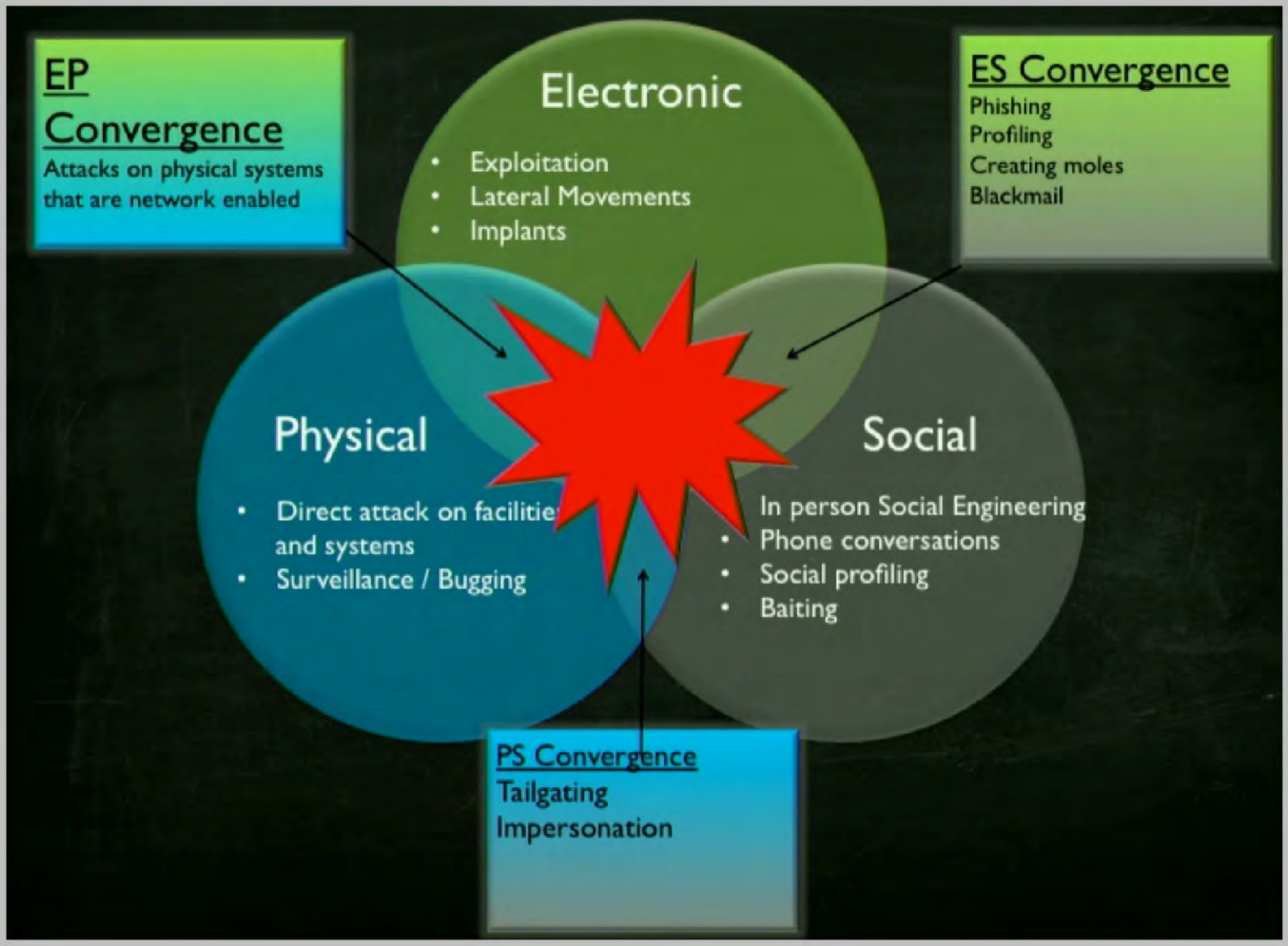
# And We Laid Hands Upon Their Server Racks



# Which Scenario Was Red Teaming?



# Some People Apply the “All Surfaces” Litmus Test



# Story Number One: Elevator Repair



# I Walked Into A Building and Hid



# I Encountered Security



# I Offered My Cover Identity and Showcased Skills

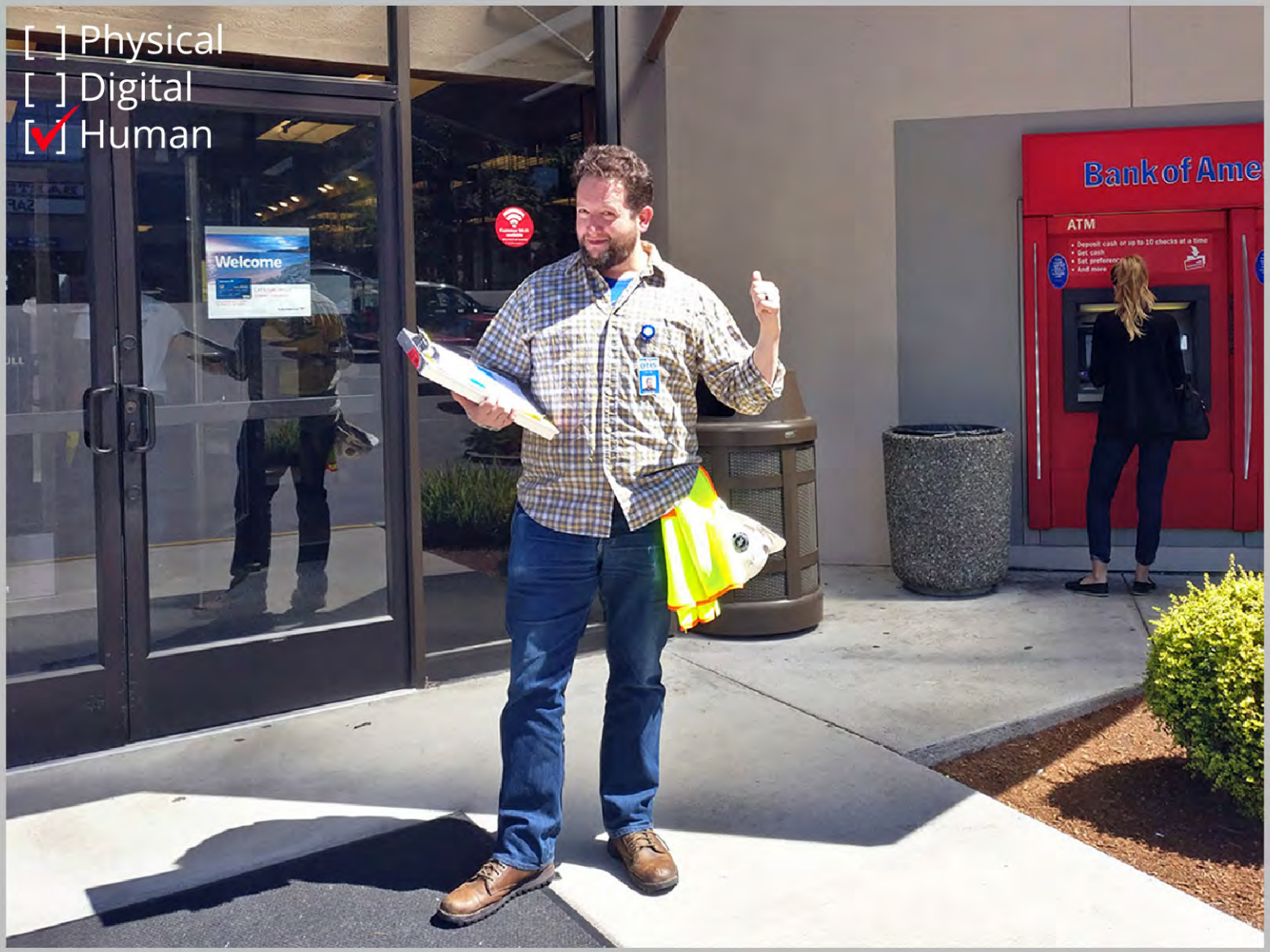
[ ] Physical
[ ] Digital
[✓] Human



# I Was Granted Escorted Access Everywhere



# I'd Call This Social Engineering



# Was This a Red Team Engagement?

[ ] Physical
[ ] Digital
[✓] Human





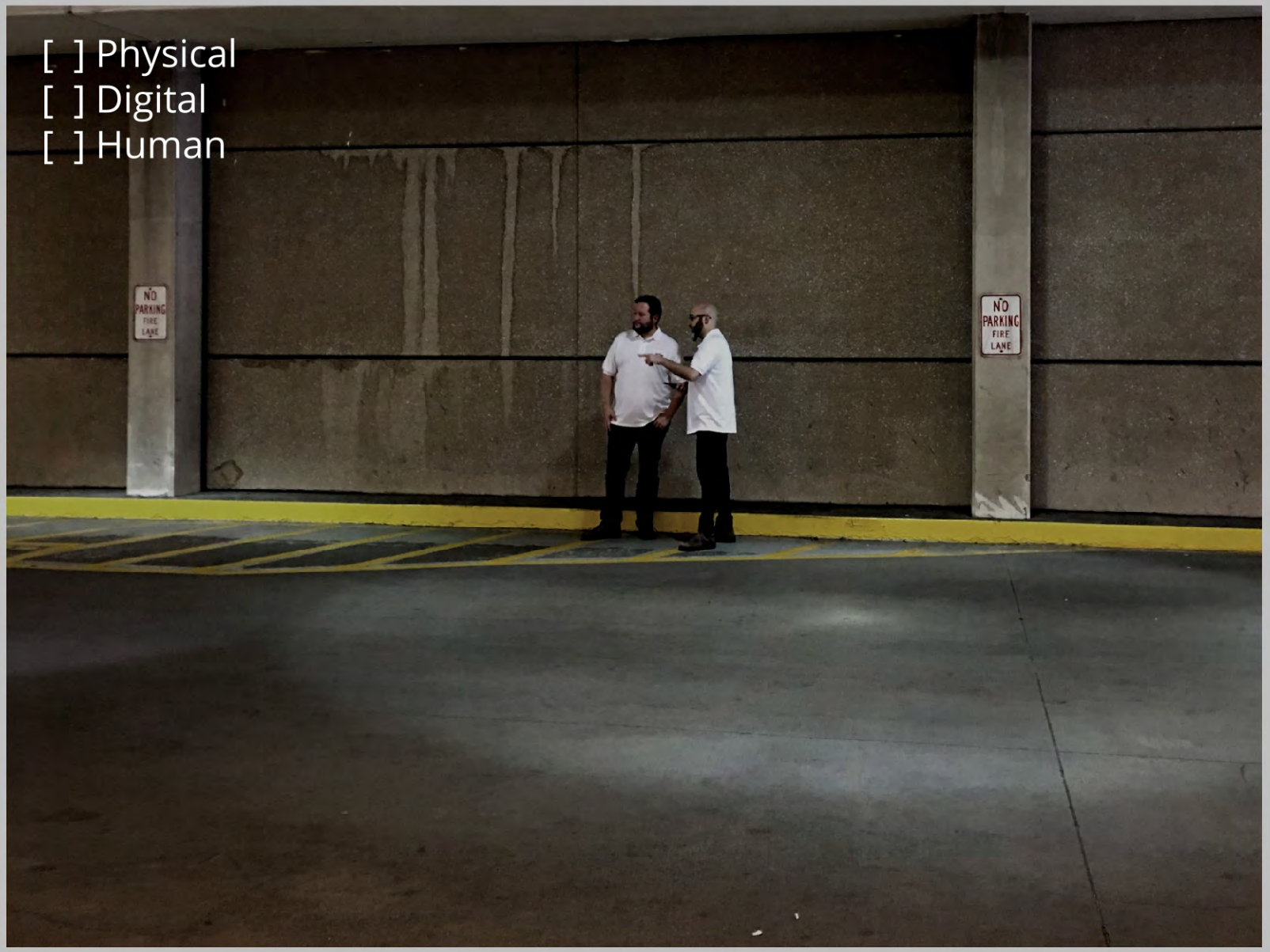
Nooooooo,

Noooooooooo...

# Story Number Two: The Cable Technicians



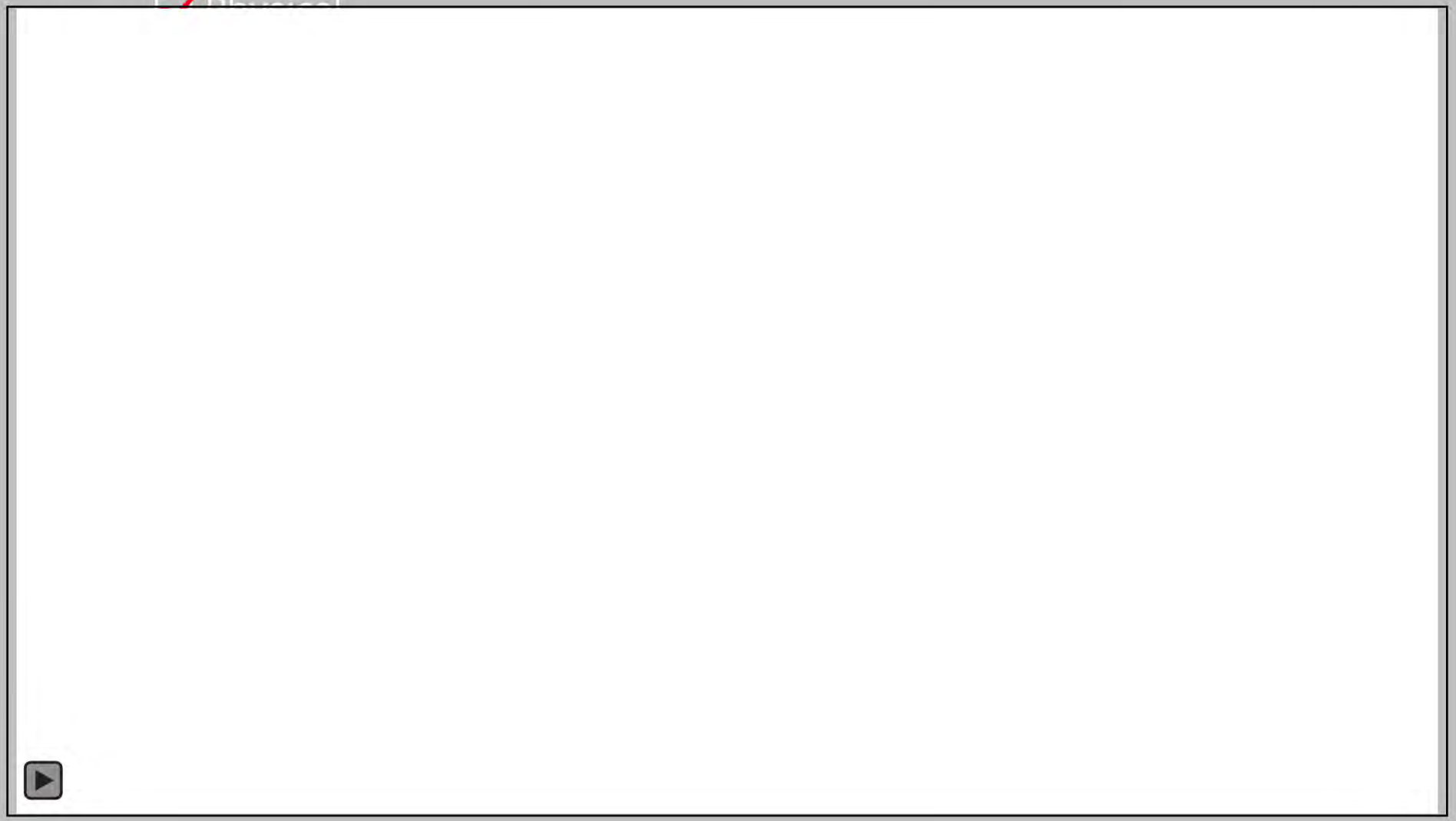
# We Spotted a Guard



# We Befriended a Guard



# We Bypassed a Door Lock

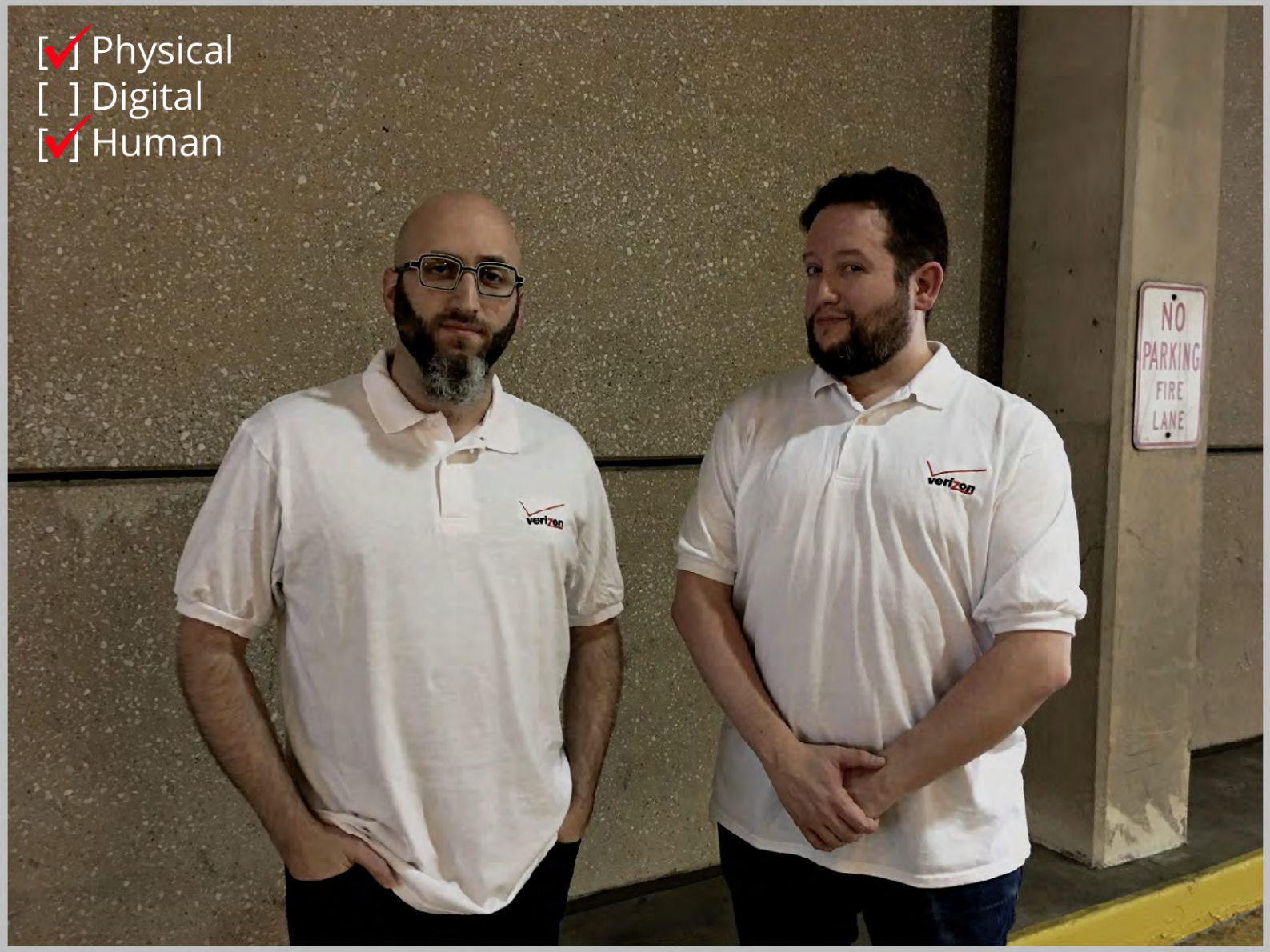


# We Bypassed Another Door

[✓] Physical
[ ] Digital
[✓] Human



# A Blended Attack... On Two Surfaces



# Was This a Red Team Engagement?




HOW ABOUT NO?

# Story Number Three: The Armed Guards



# We Prepared a HuntPad



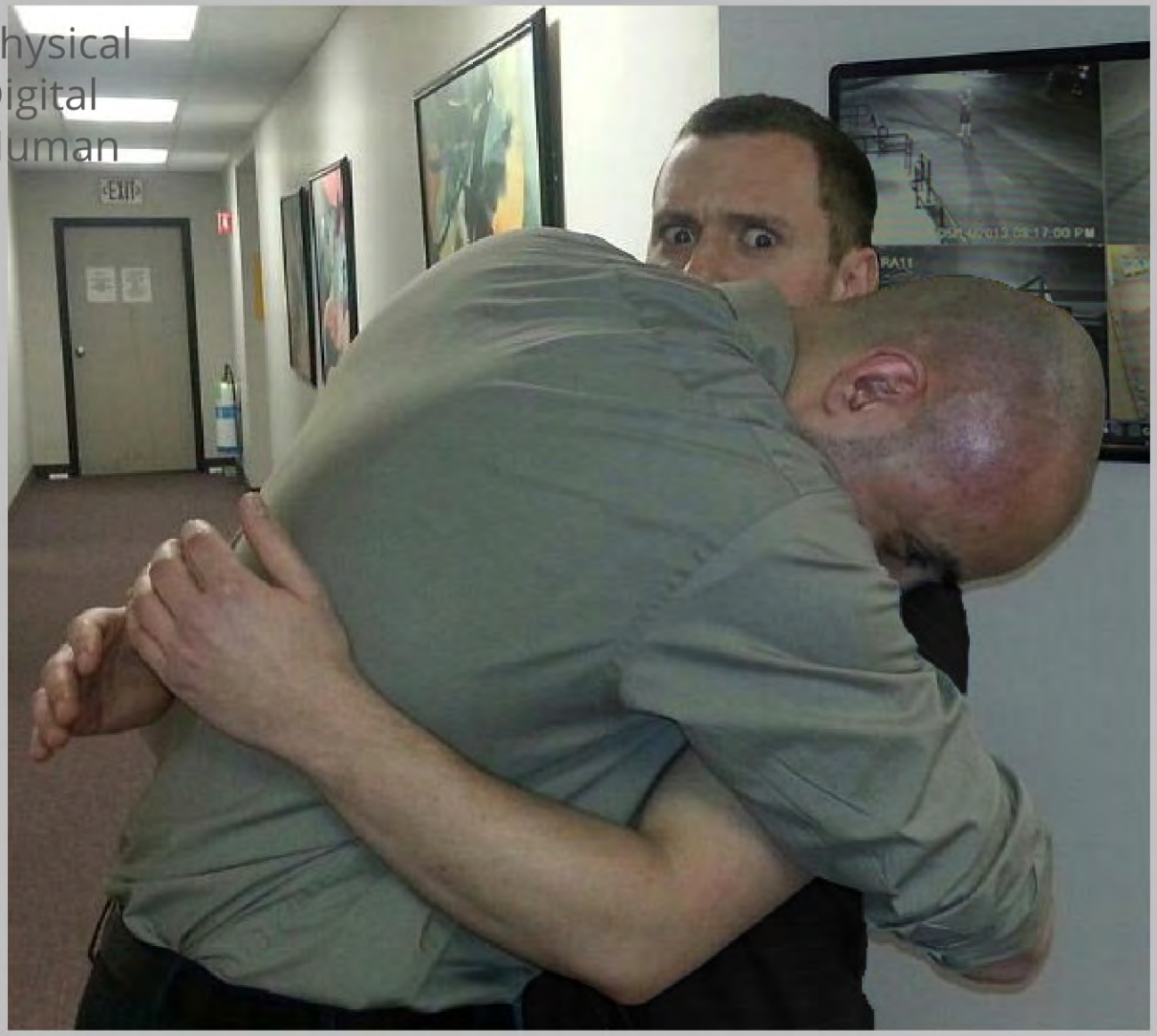
# We Established Rapport

[ ] Physical
[ ] Digital
[✓] Human

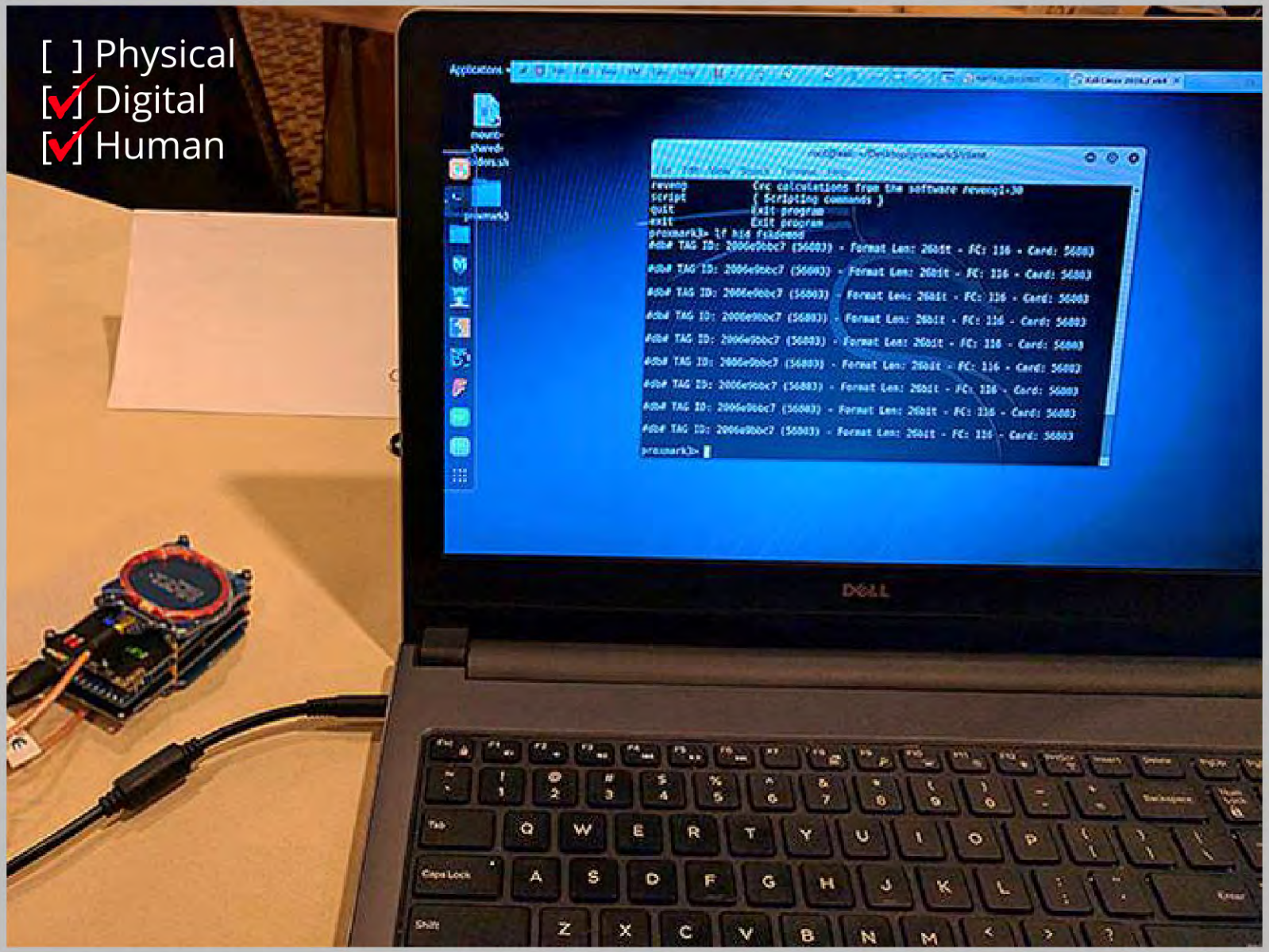


# We Grabbed RFID Card Data

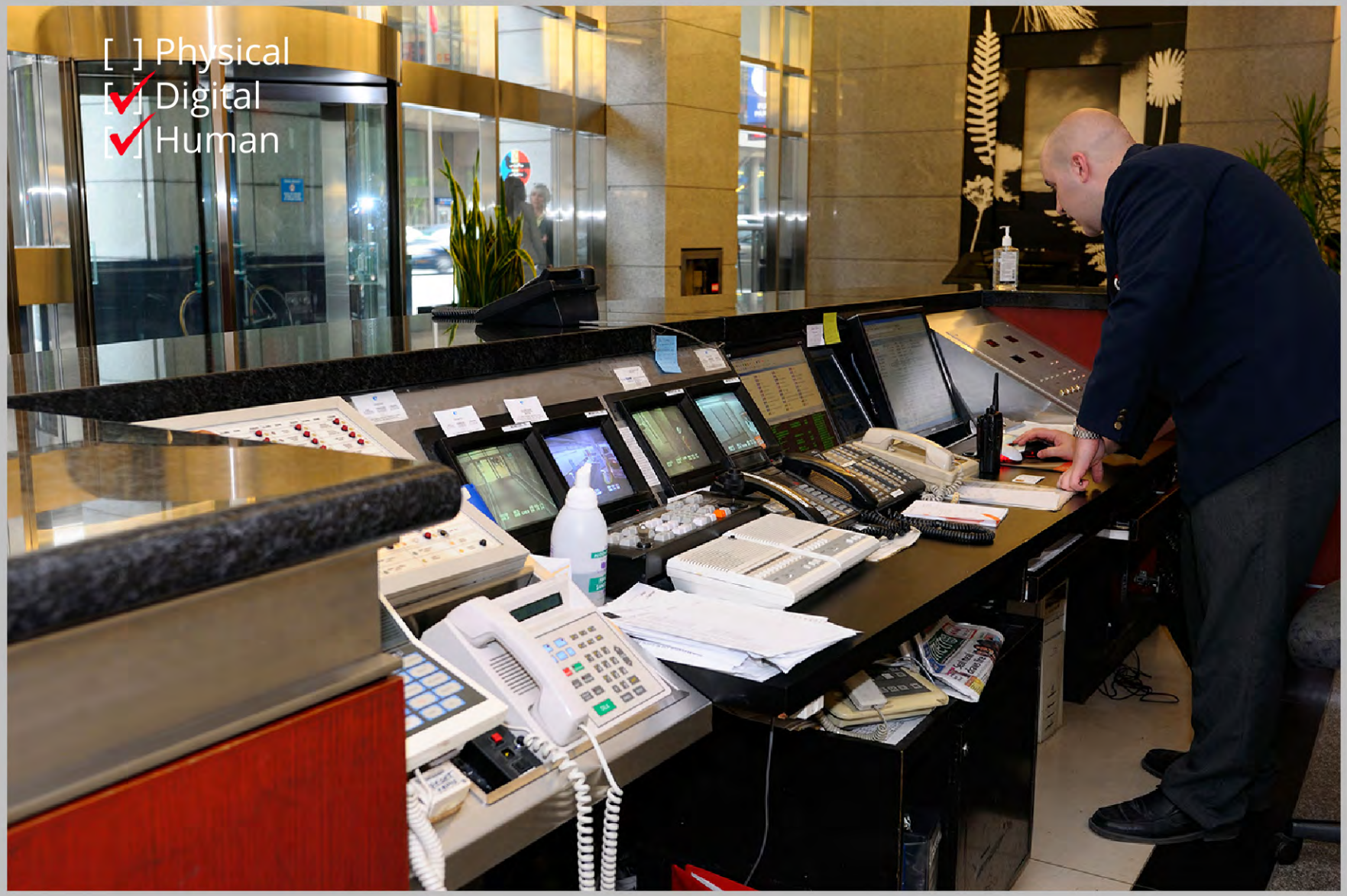
[ ] Physical
[✓] Digital
[✓] Human



# We Wrote New Badge Data



# We Bluffed Past More Guards



# We Overrode an Elevator



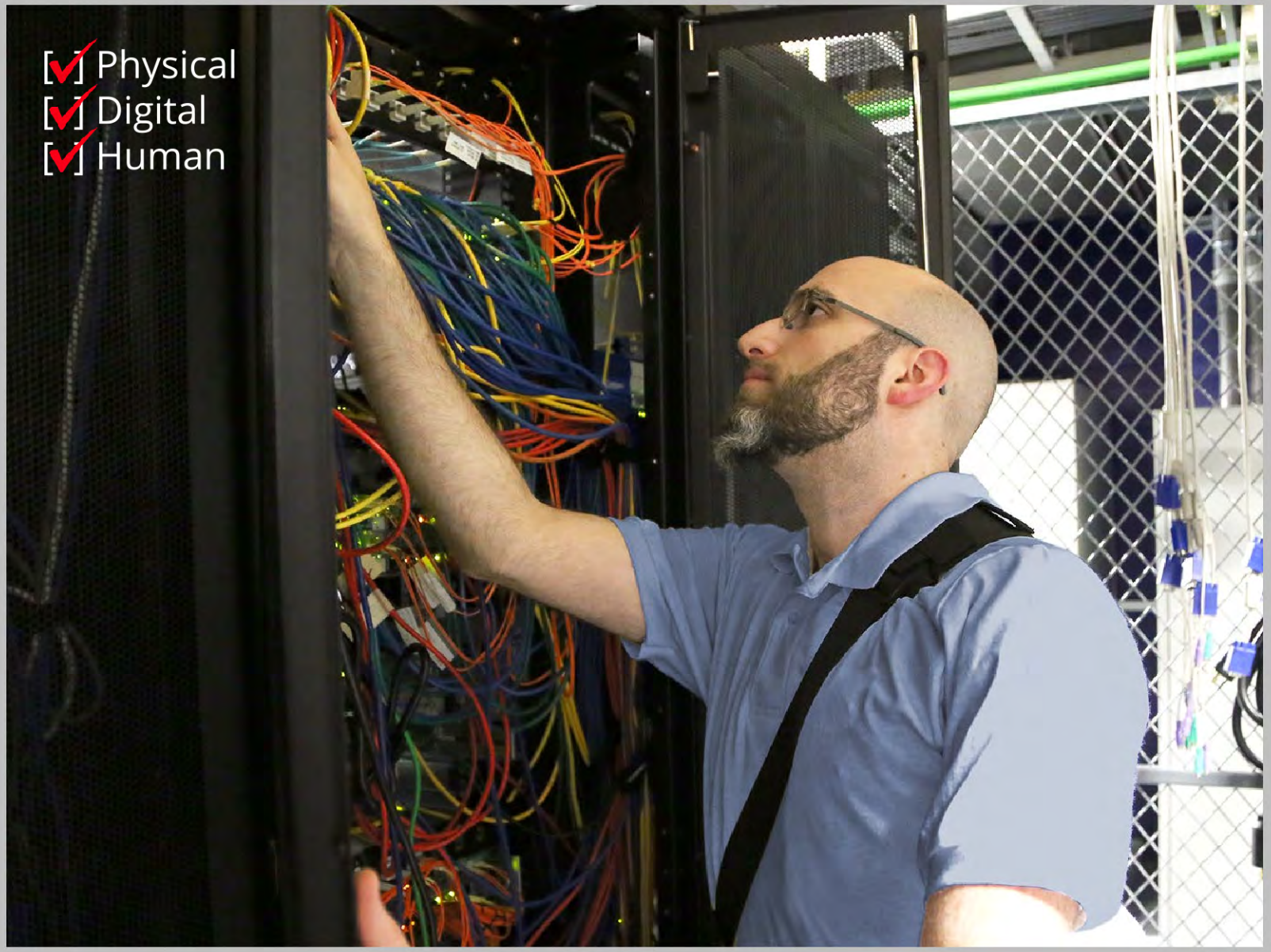
# We Picked Locks



# We Entered the Server Room

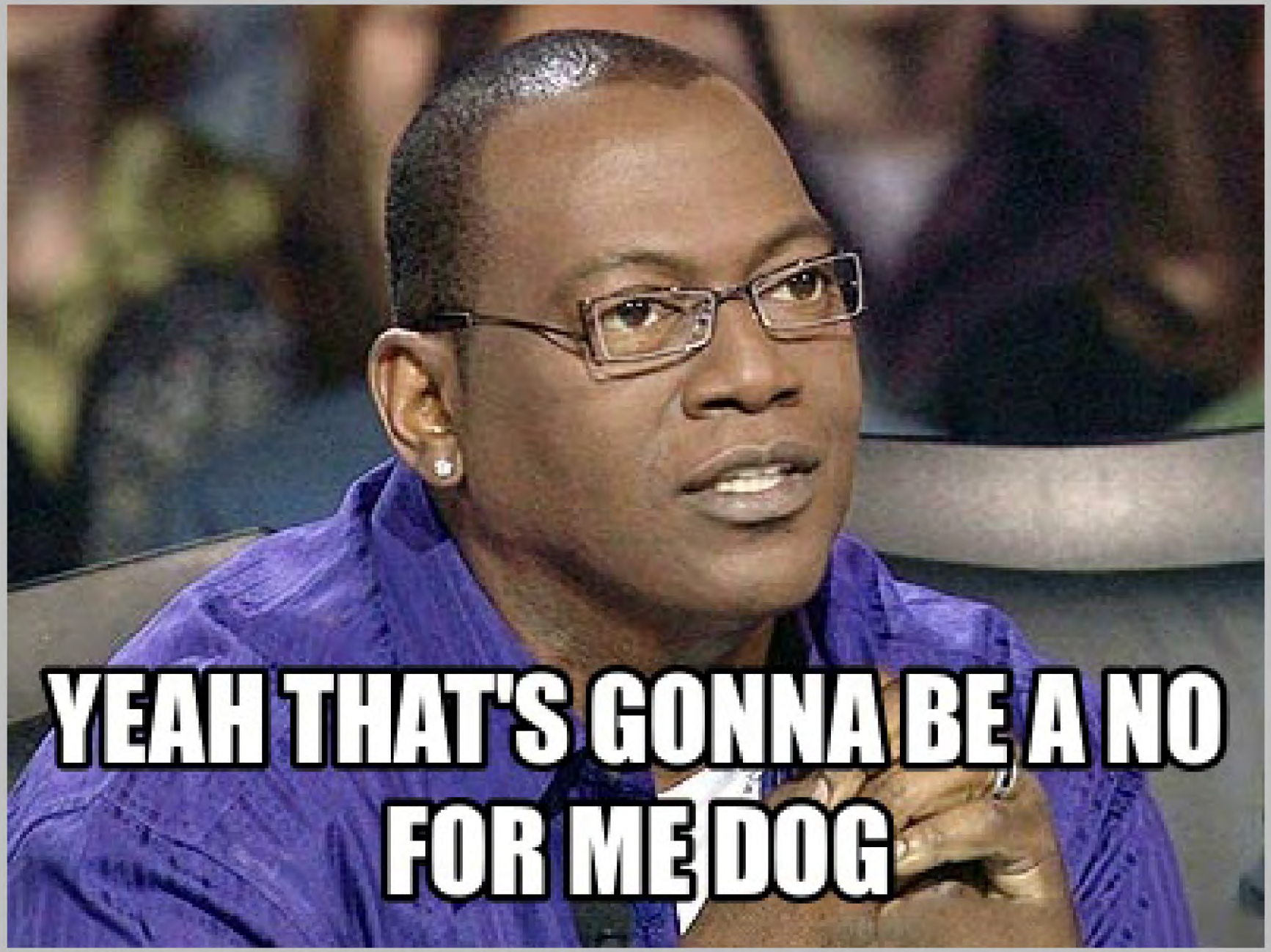


# We Feigned Network Attacks



# Was This a Red Team Engagement?




YEAH THAT'S GONNA BE A NO
FOR ME, DOG

# Ahhhh... The Question of How Much Scope







# Ahhhh... The Question of How Much Scope



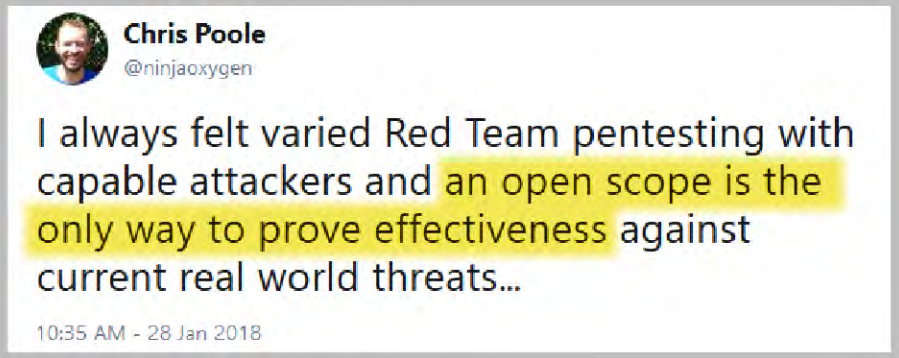


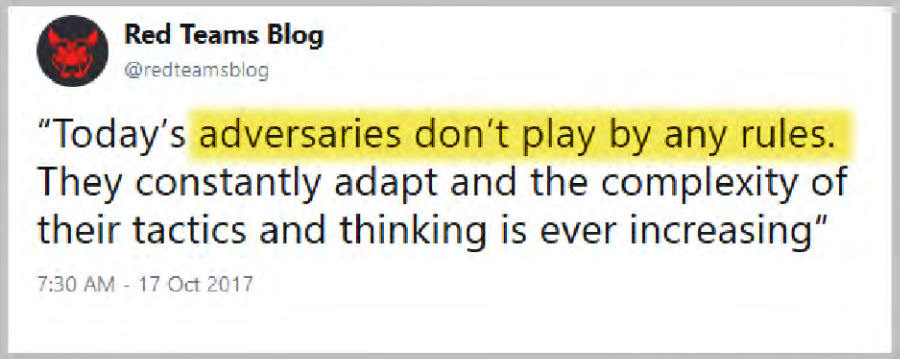


## Is *That* What Makes Something a Red Team Engagement?

# Ahhhh… The Question of How Much Scope



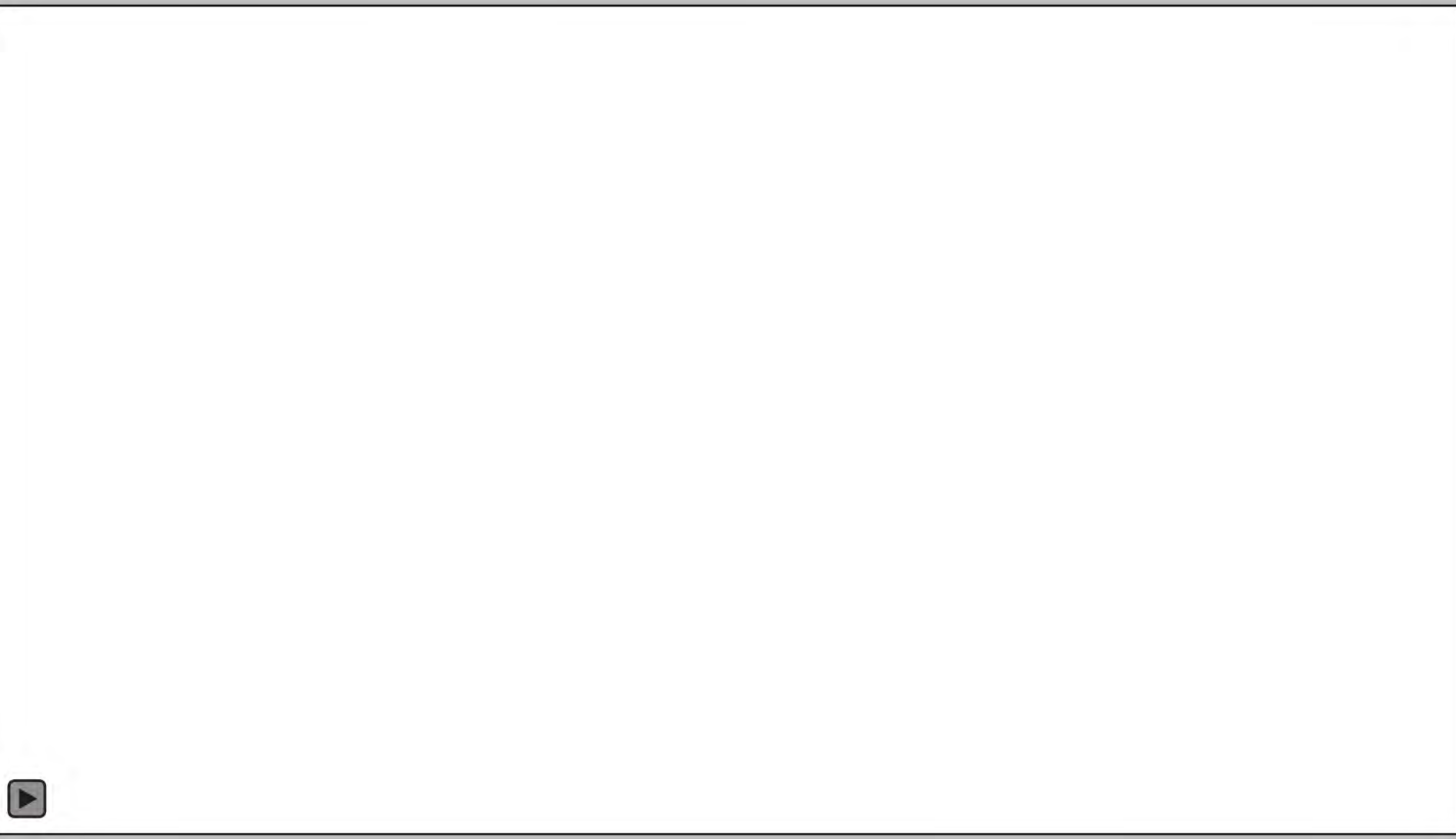



# Scope *Absolutely* Has a Place in Red Teaming



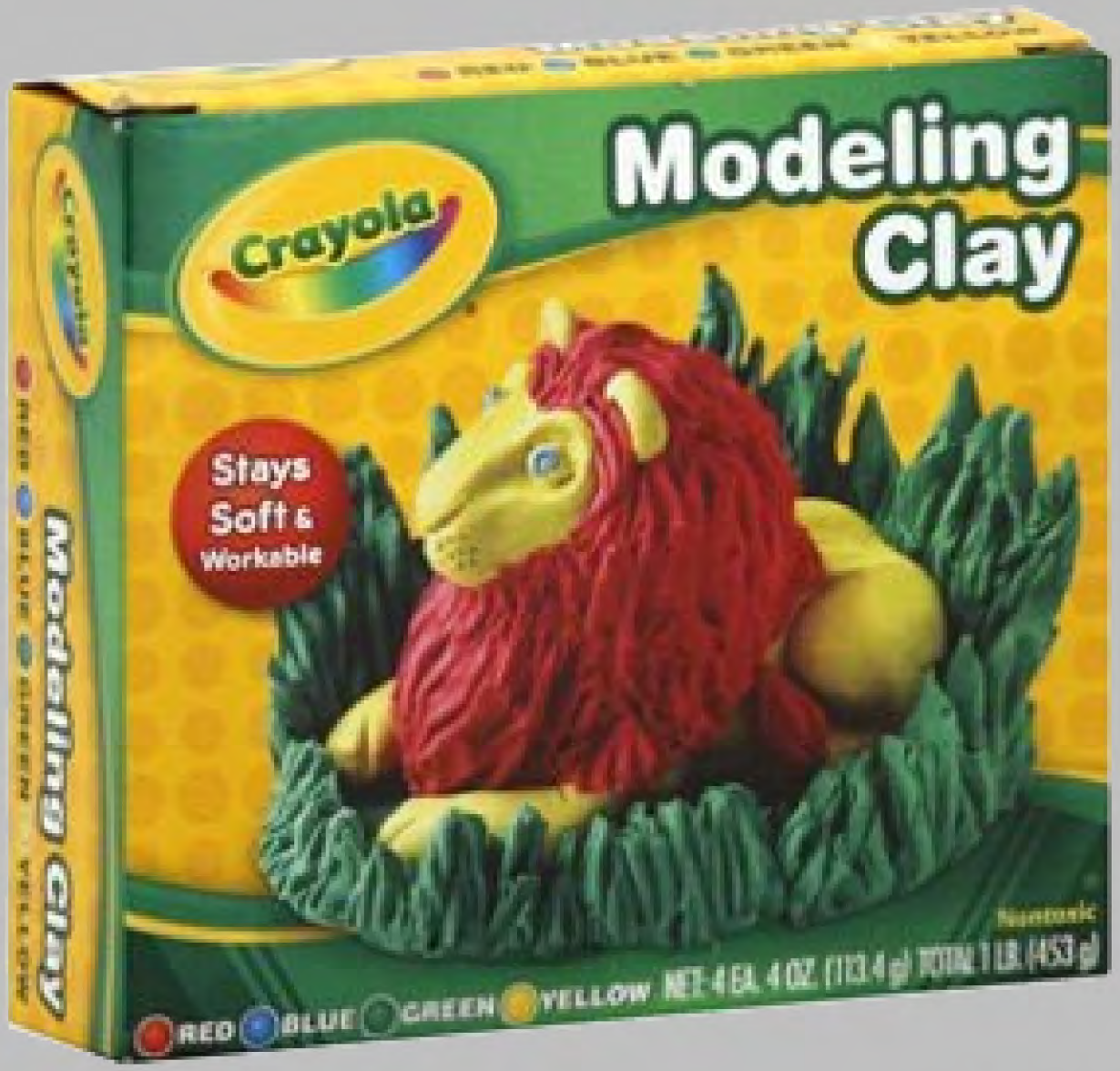
# Scope *Absolutely* Has a Place in Red Teaming



# Stop Thinking You Know More Than The Client



# What Threat Are You Being Hired To Model?



# What Do Clients Ultimately Care About?



# What Do Clients Ultimately Care About?



Is a Given Vulnerability Going To...

1. Cost Me Money

2. Make Me Look Bad

# “Cost Me Money”



# “Make Me Look Bad”



# (Many Times the Two are Related)



# Your Job as a Red Teamer...



# Your Job as a Red Teamer...

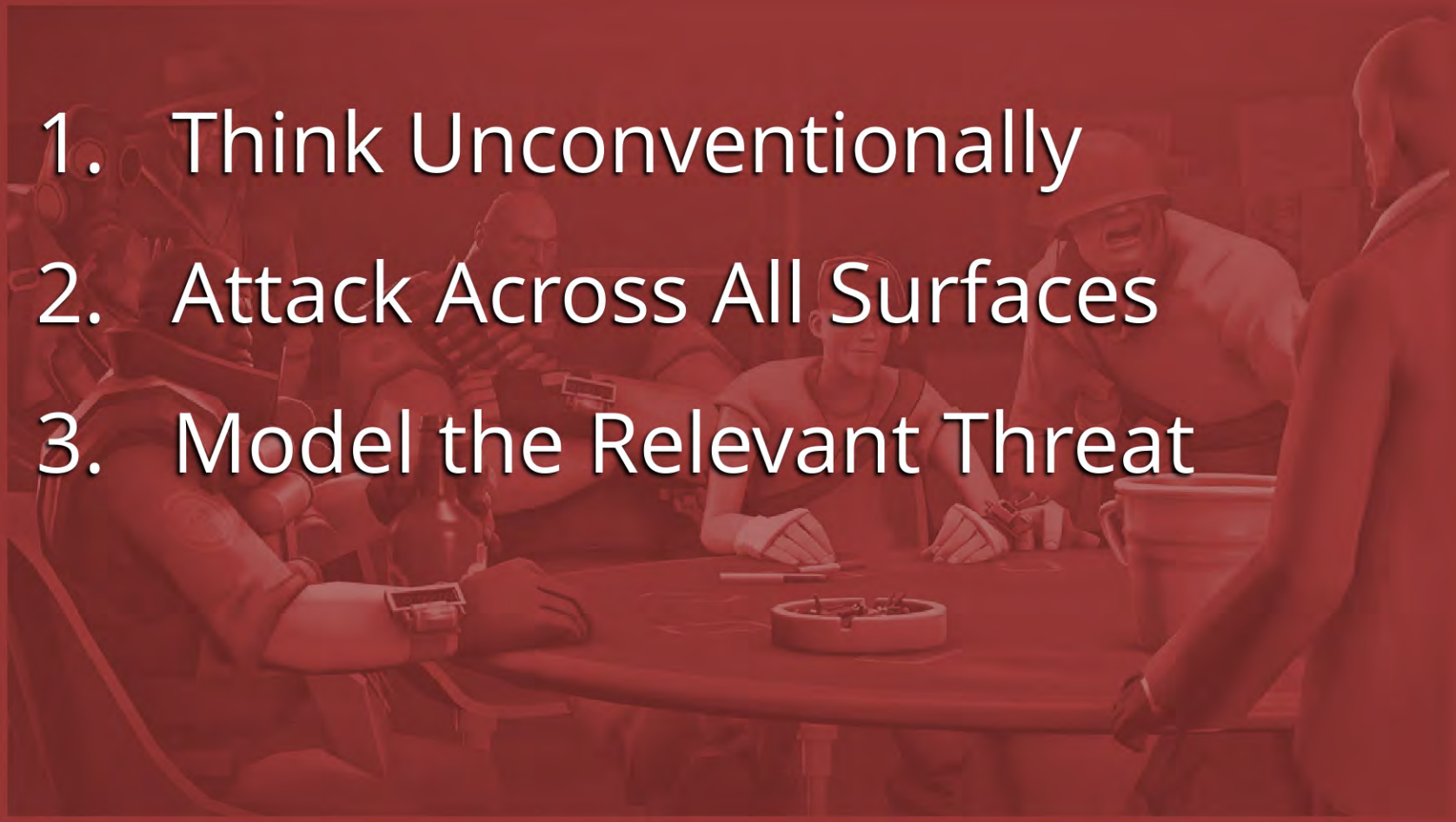


# Your Job as a Red Teamer...



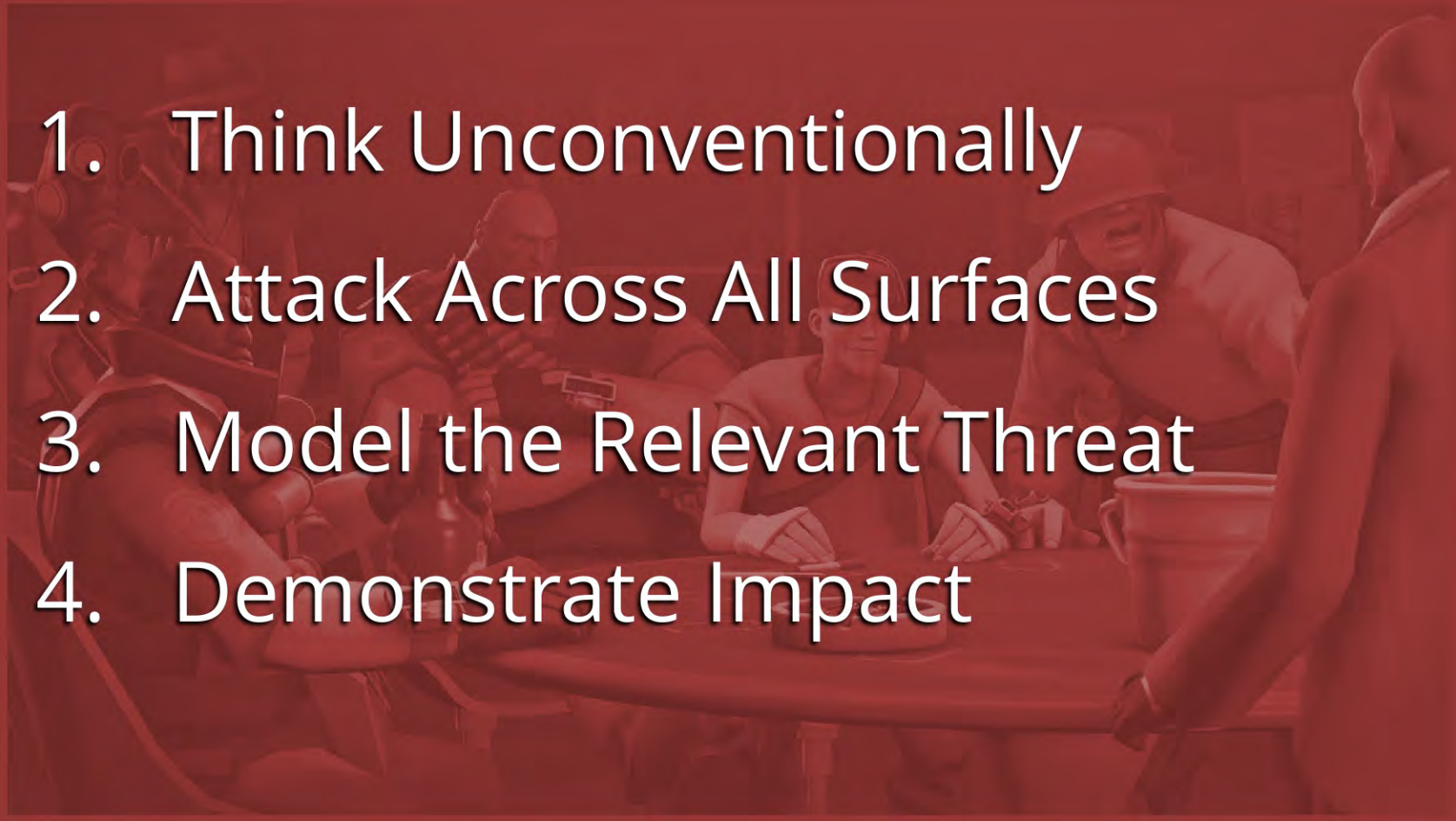
1. Think Unconventionally
2. Attack Across All Surfaces

# Your Job as a Red Teamer...



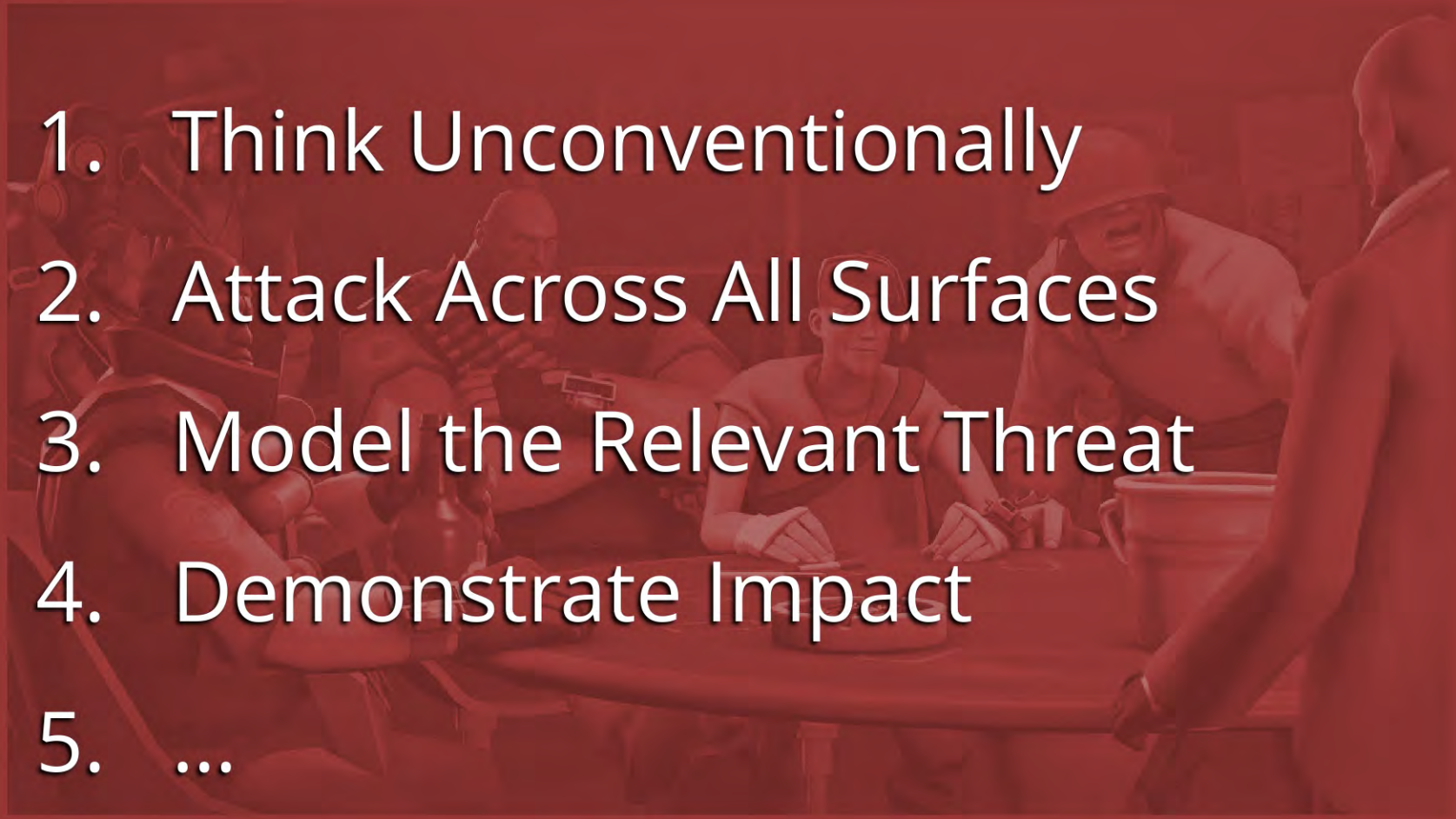
1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat

# Your Job as a Red Teamer...



1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact

# Your Job as a Red Teamer...



1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. ...

# What Else is Missing?










# Your Job as a Red Teamer...

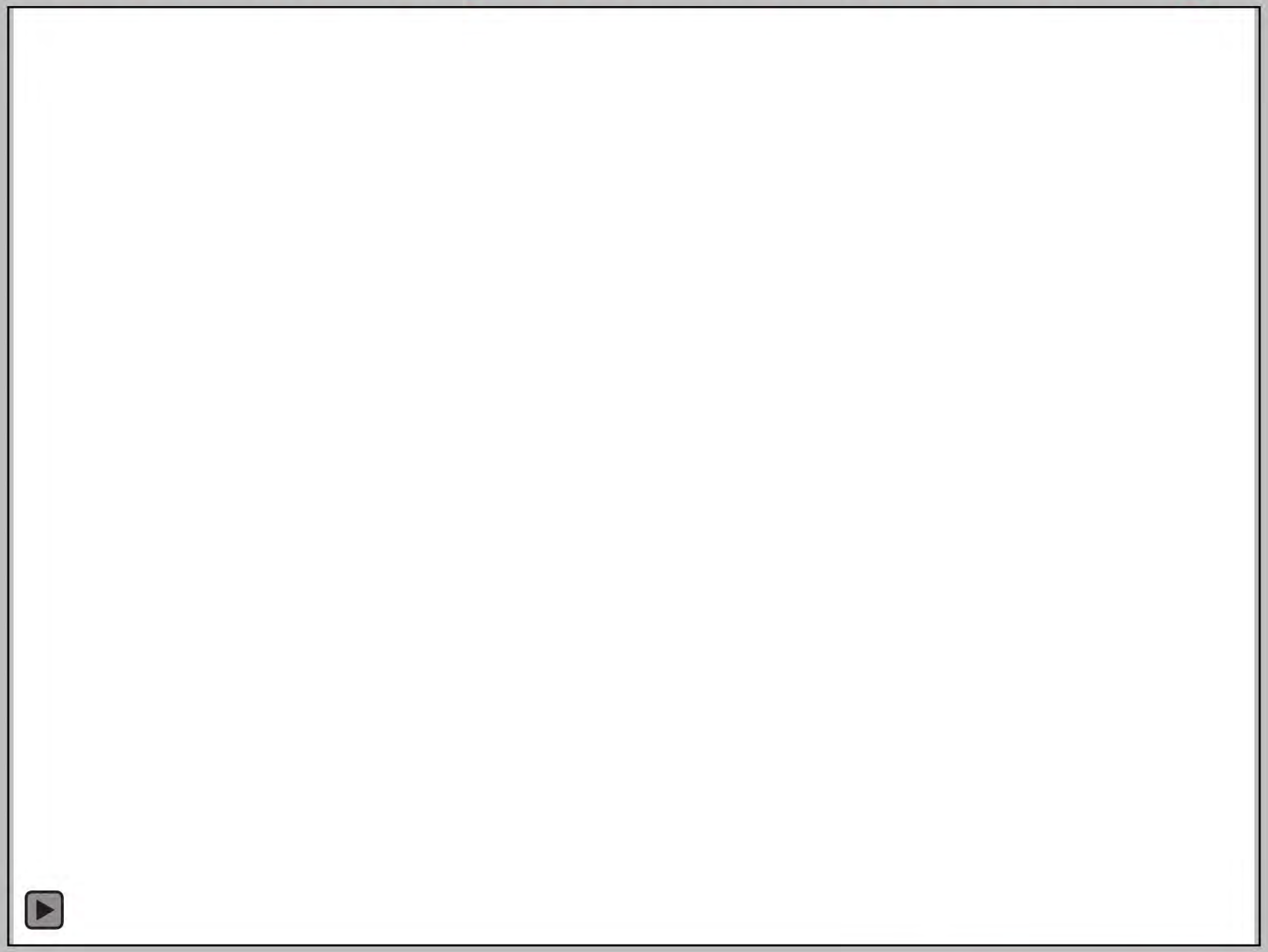


1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. Interface with the Blue Team

# I Love the Sparring Analogy



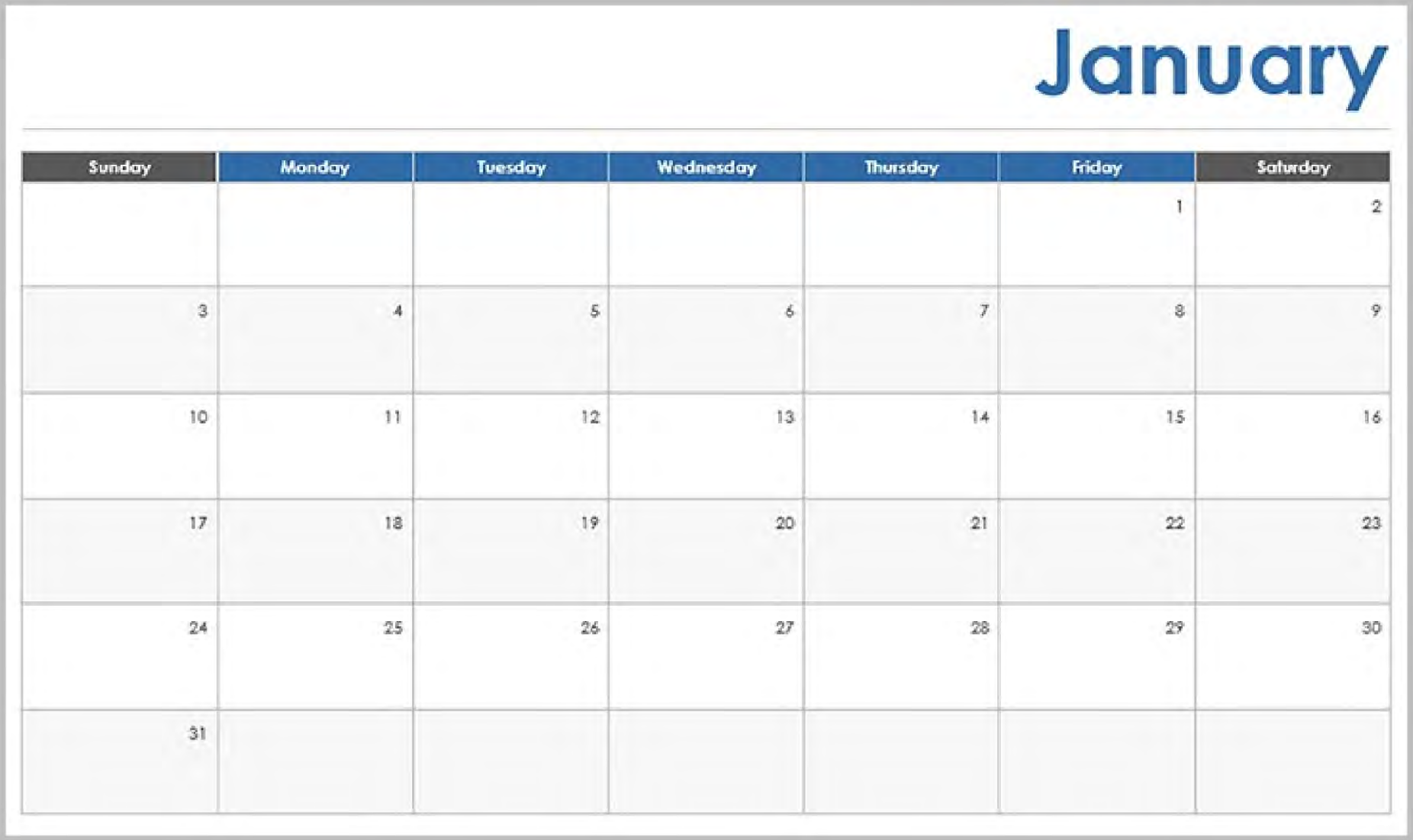
# This is What Many Folk Think “Red Teaming” Is



# This is What You Want to Eventually See



# Build This Into Your Jobs



# Build This Into Your Jobs



# Build This Into Your Jobs

## January

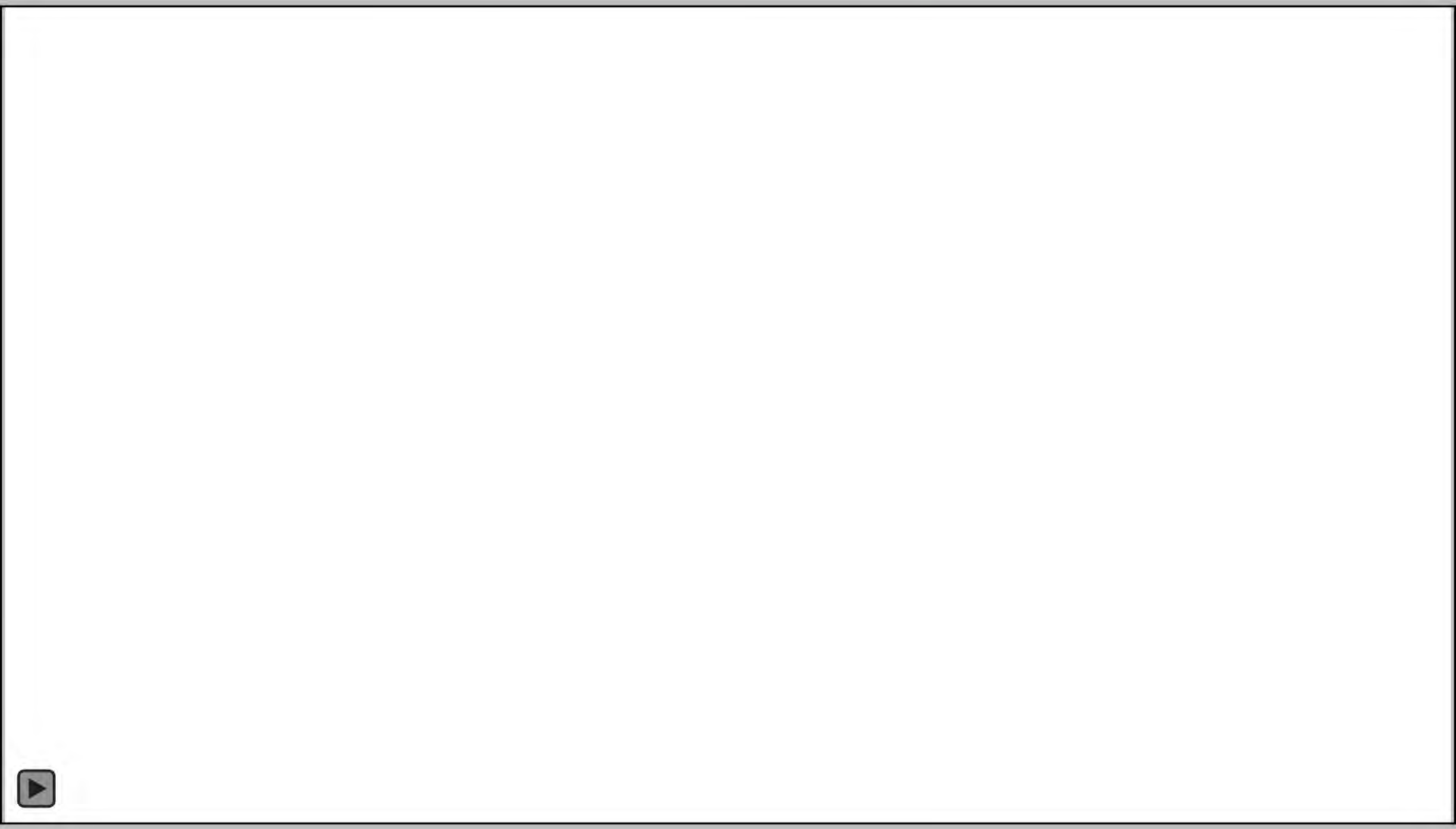
| Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | Last Job Ran Long | Laundry & Repack |
| Research the Target While Flying There | Wreck Shit | Wreck Shit | Wreck Shit | Hustle to Next Job | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | | |

# Build This Into Your Jobs

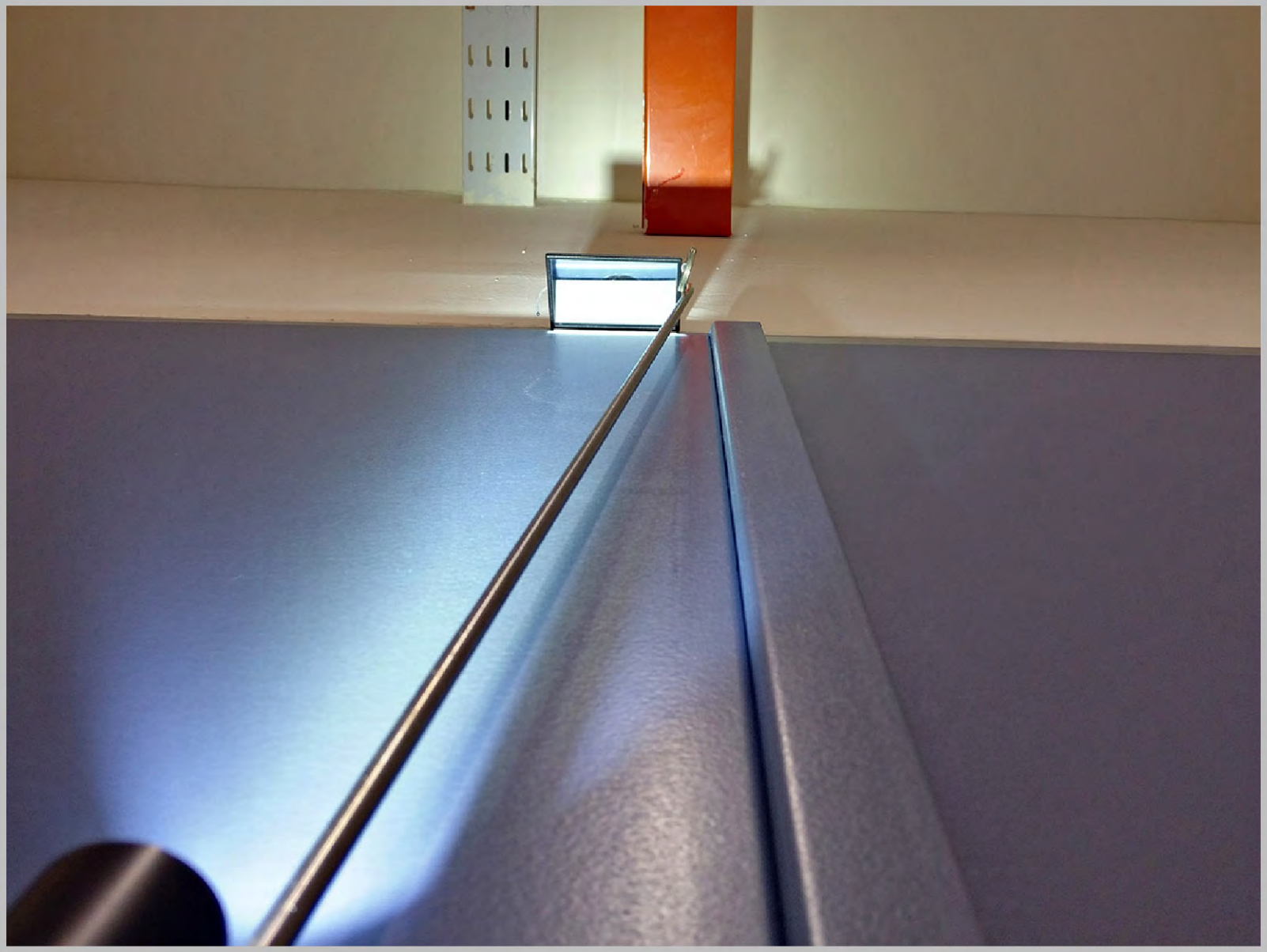
## January

| Sunday | Monday | Tuesday | Wednesday | Thursday | Friday | Saturday |
|---|---|---|---|---|---|---|
| | | | | | 1 | 2 |
| 3 | 4 | 5 | 6 | Recon | Recon | Plan & Prep |
| Achieve Objectives | Achieve Objectives | Achieve Objectives | Achieve Objectives | **After-Action Meetings** | **Practice w/ Blue Team** | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | | | | | | |

# Real-World Examples



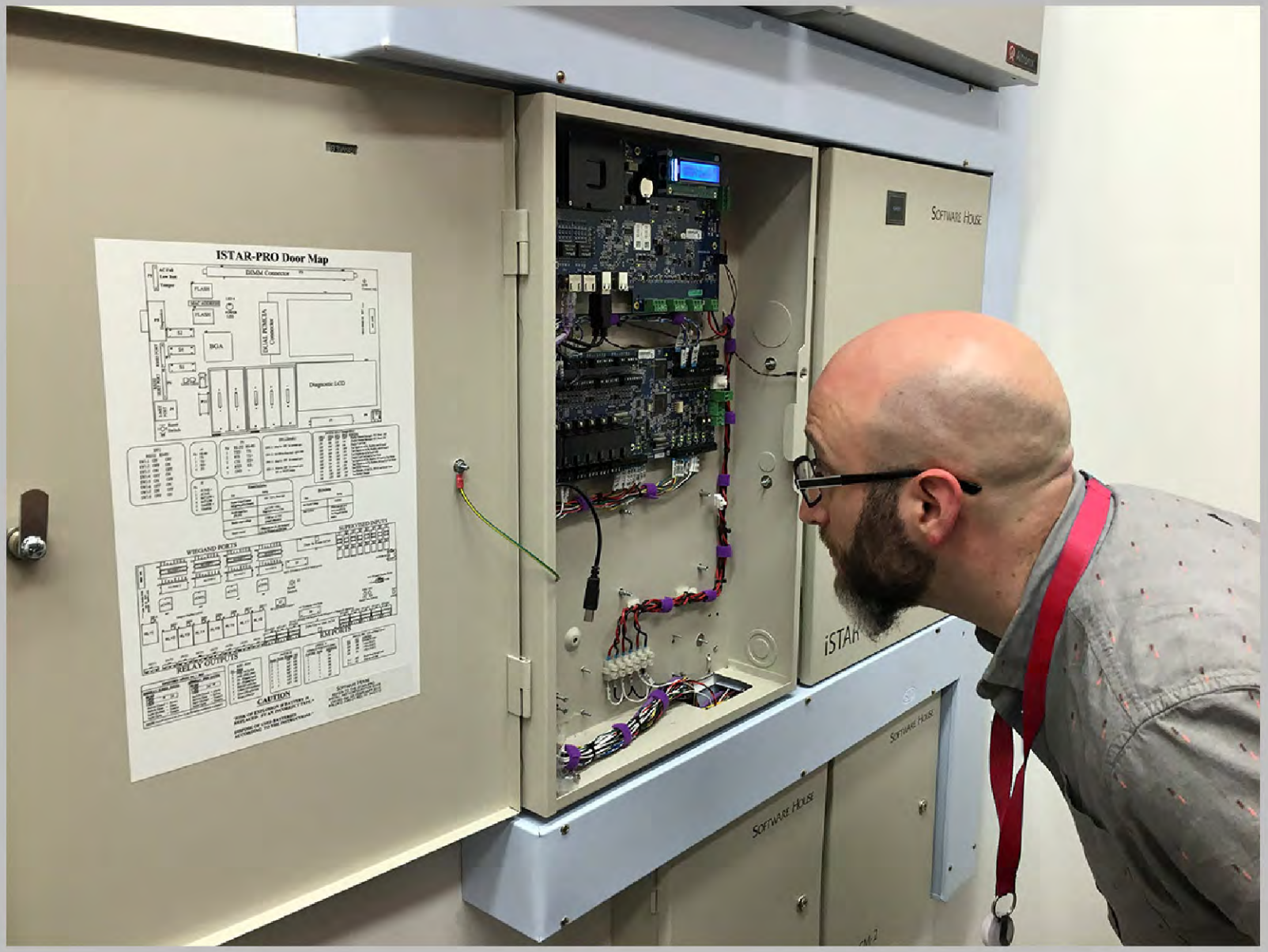
# Real-World Examples



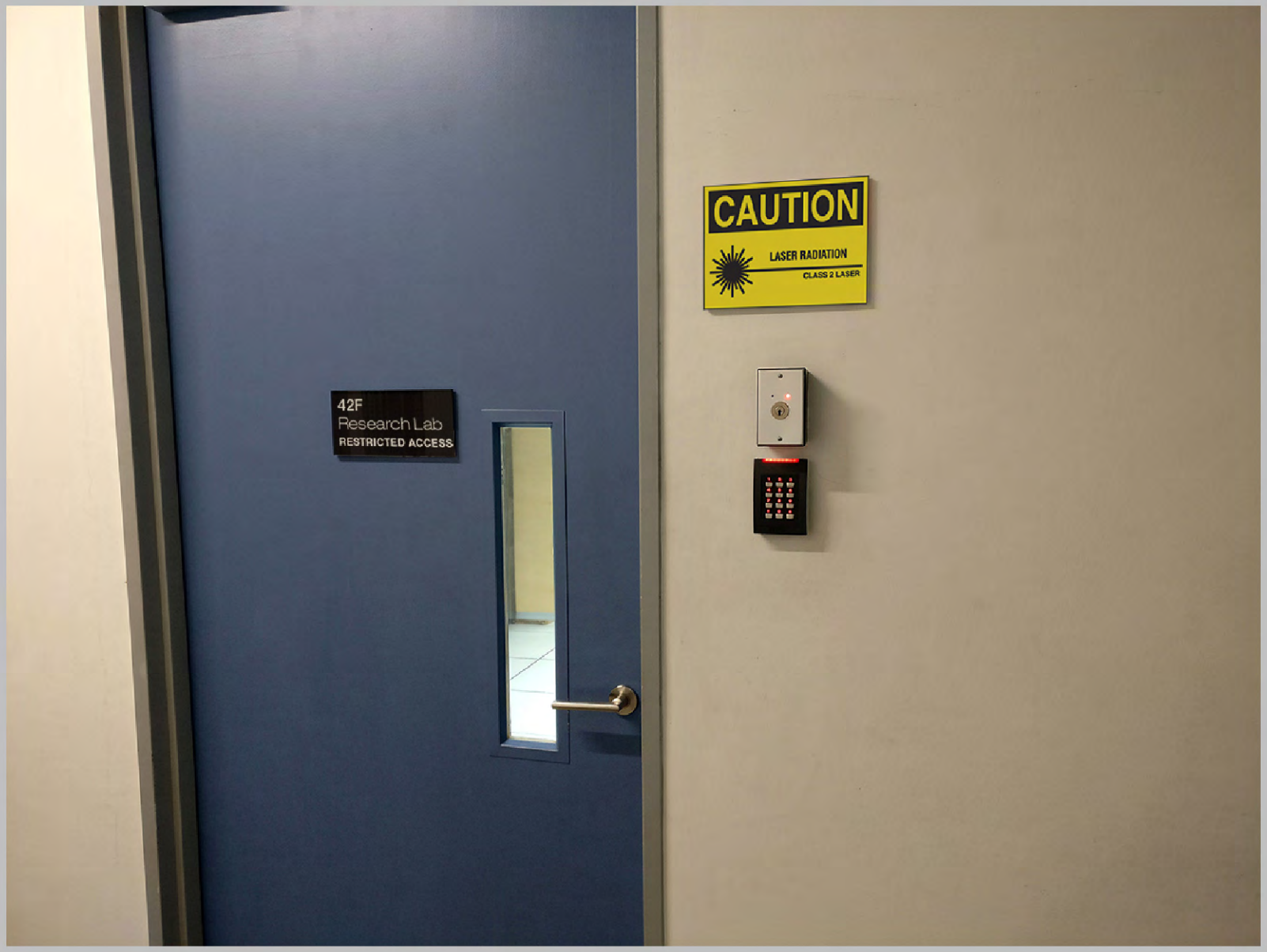
# Real-World Examples



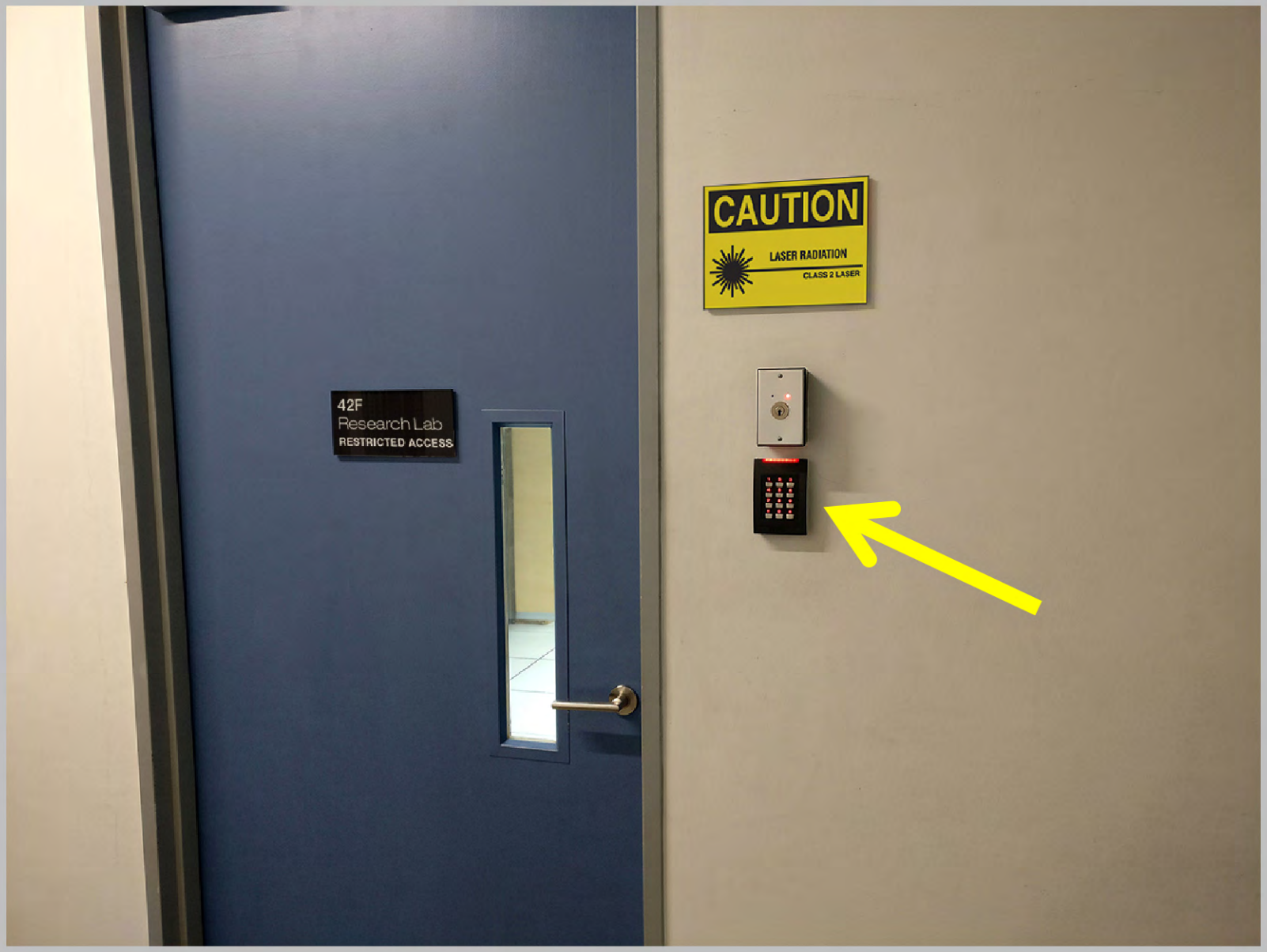
# Real-World Examples



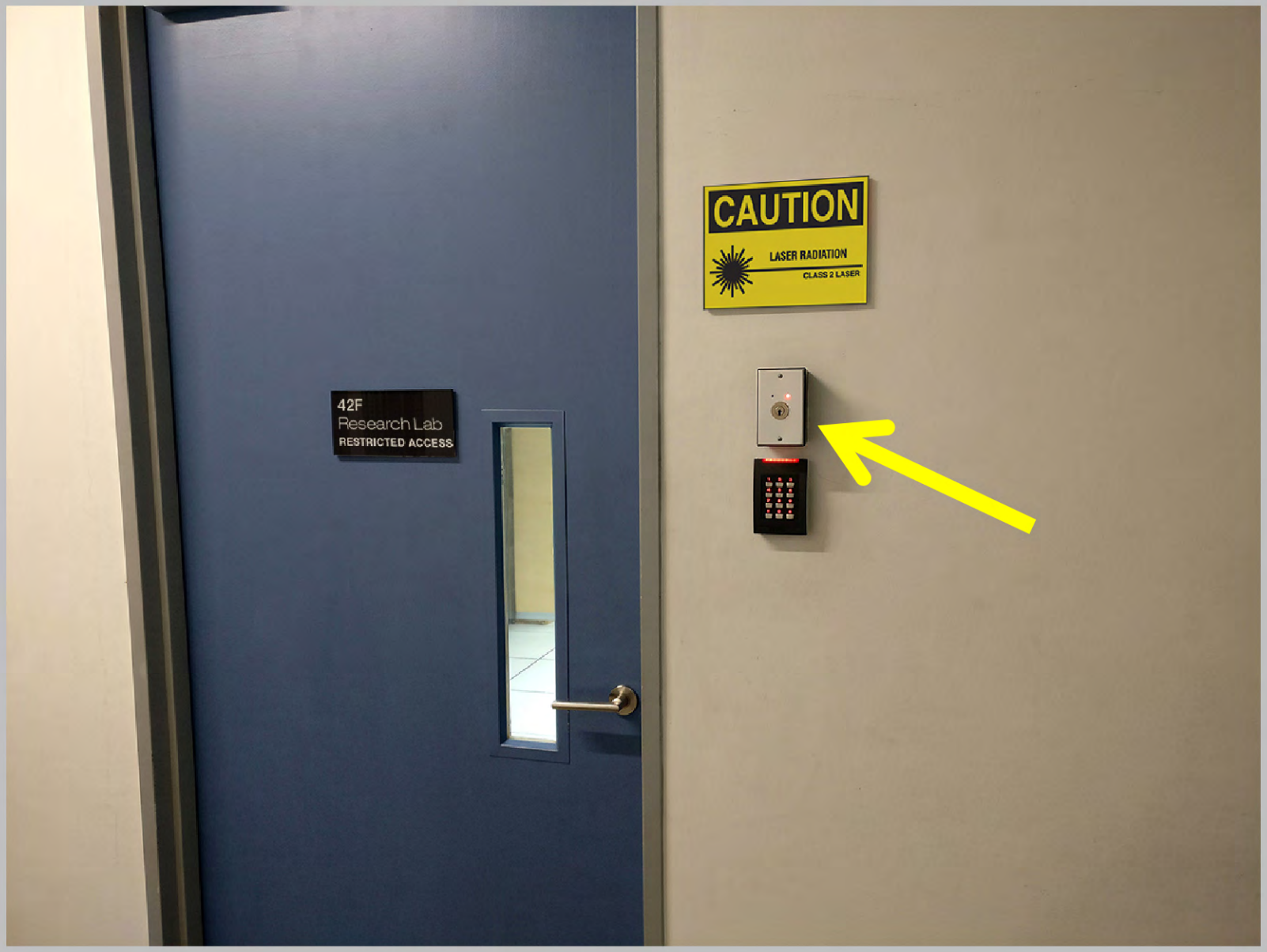
# Real-World Examples



# Real-World Examples



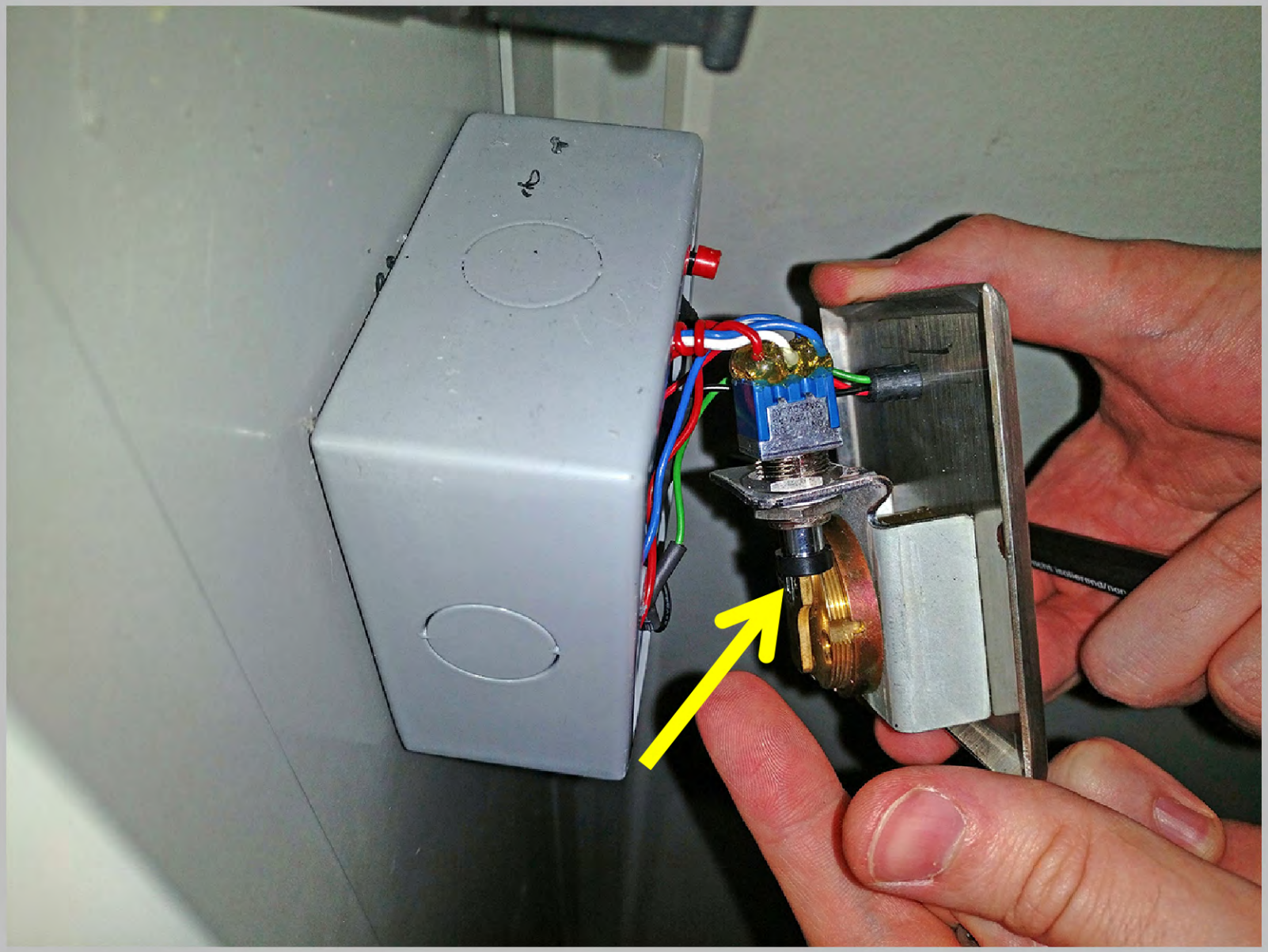
# Real-World Examples



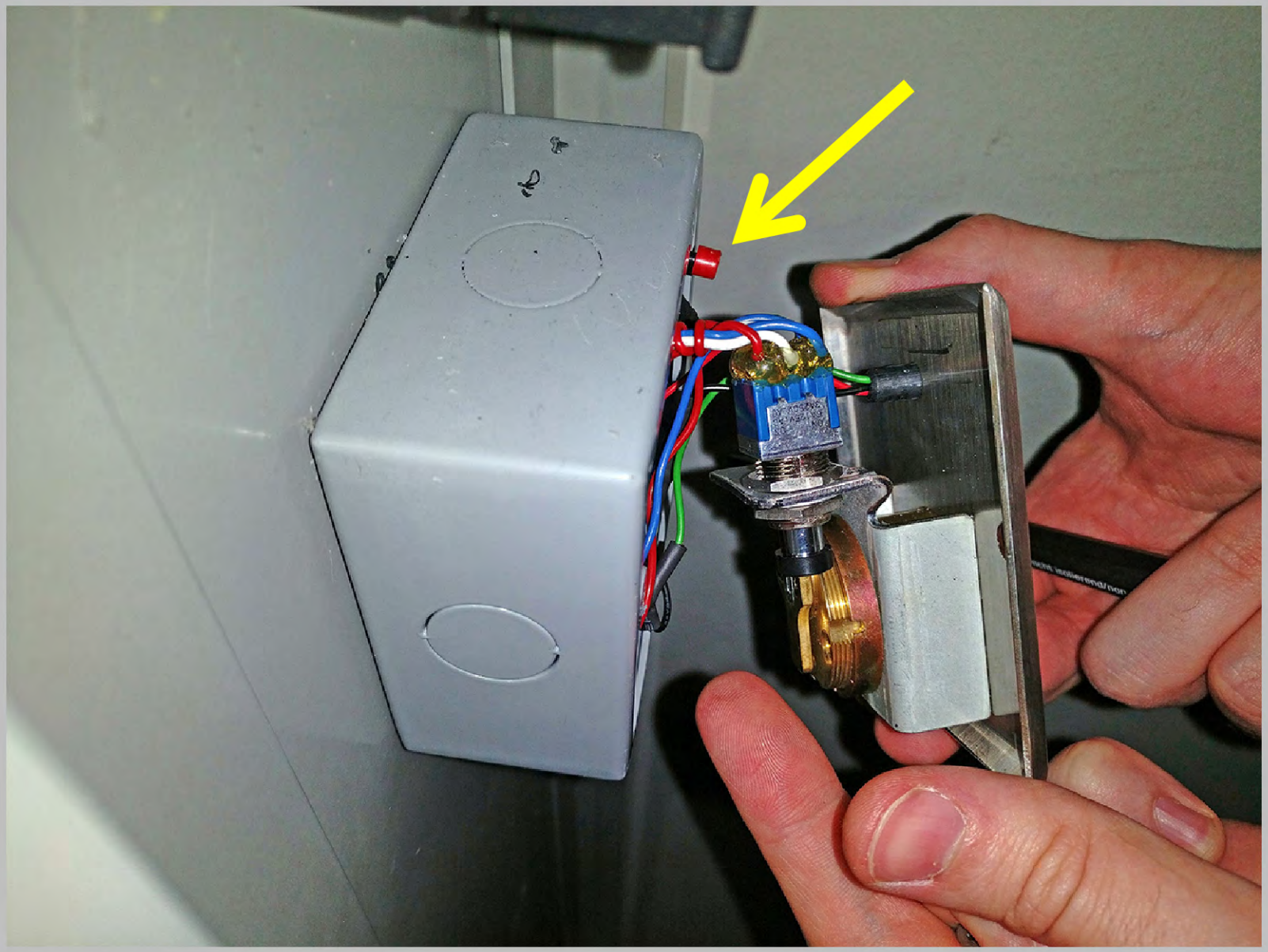
# Real-World Examples



# Real-World Examples



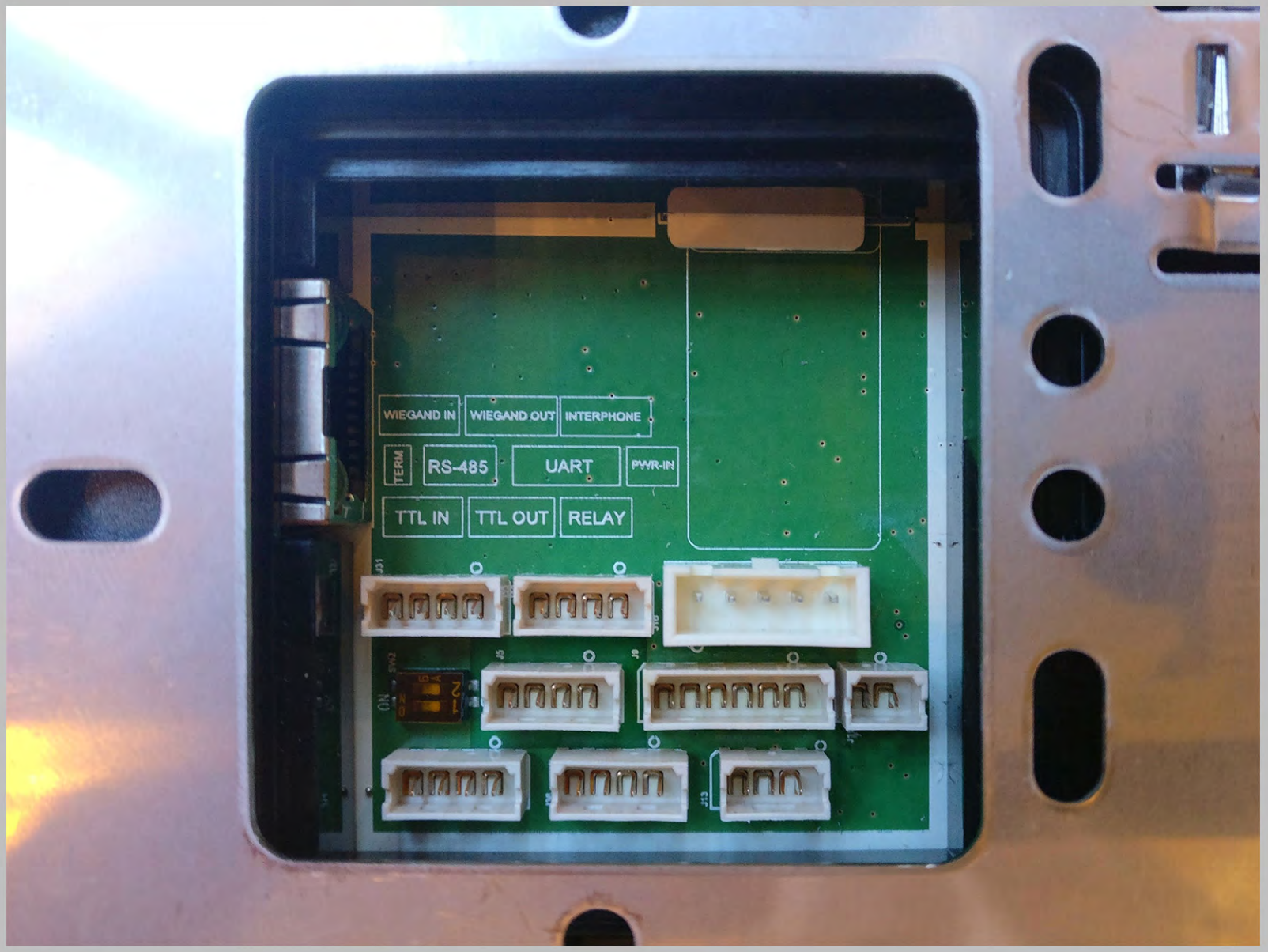
# Real-World Examples



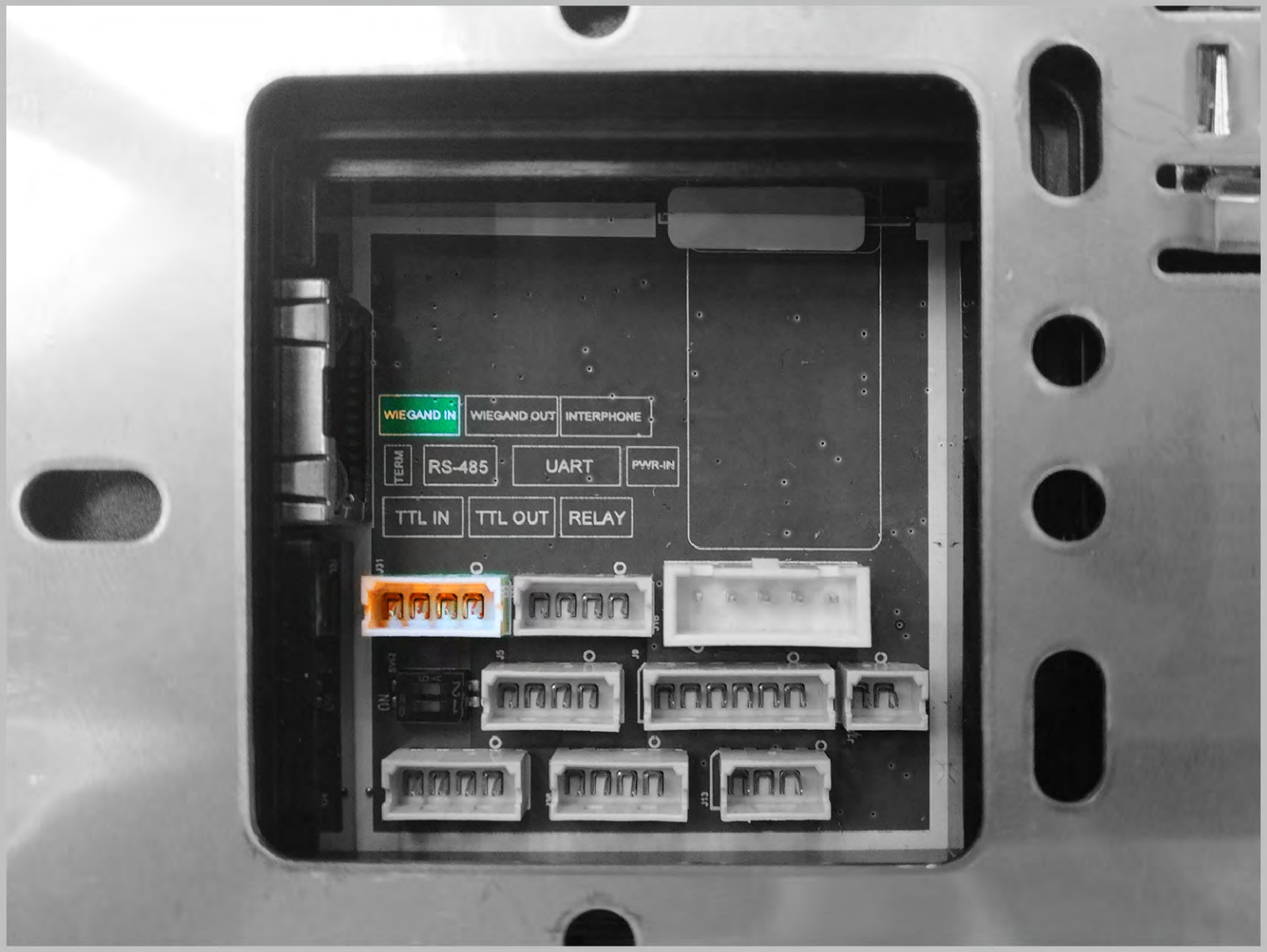
# Real-World Examples



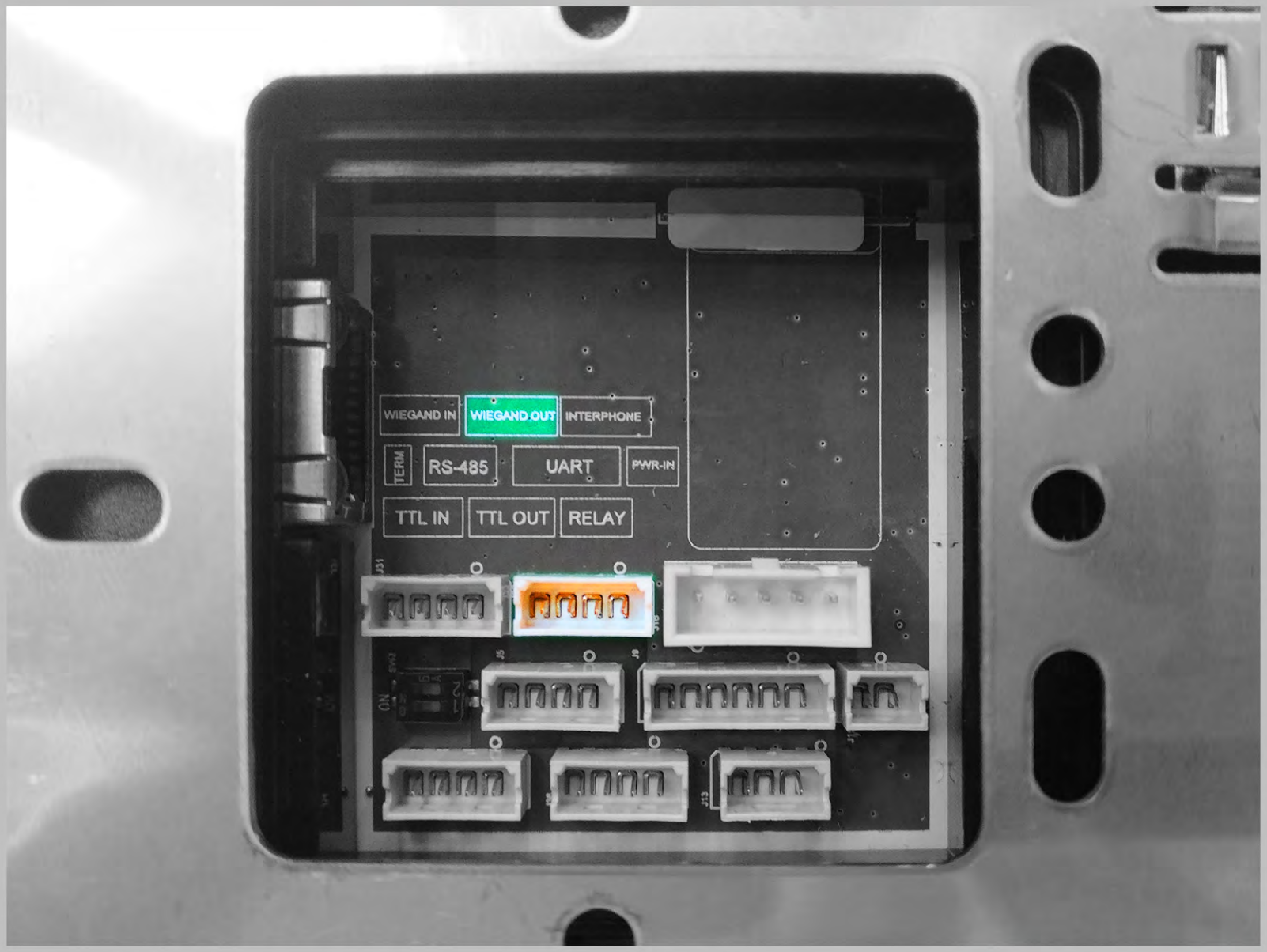
# Real-World Examples



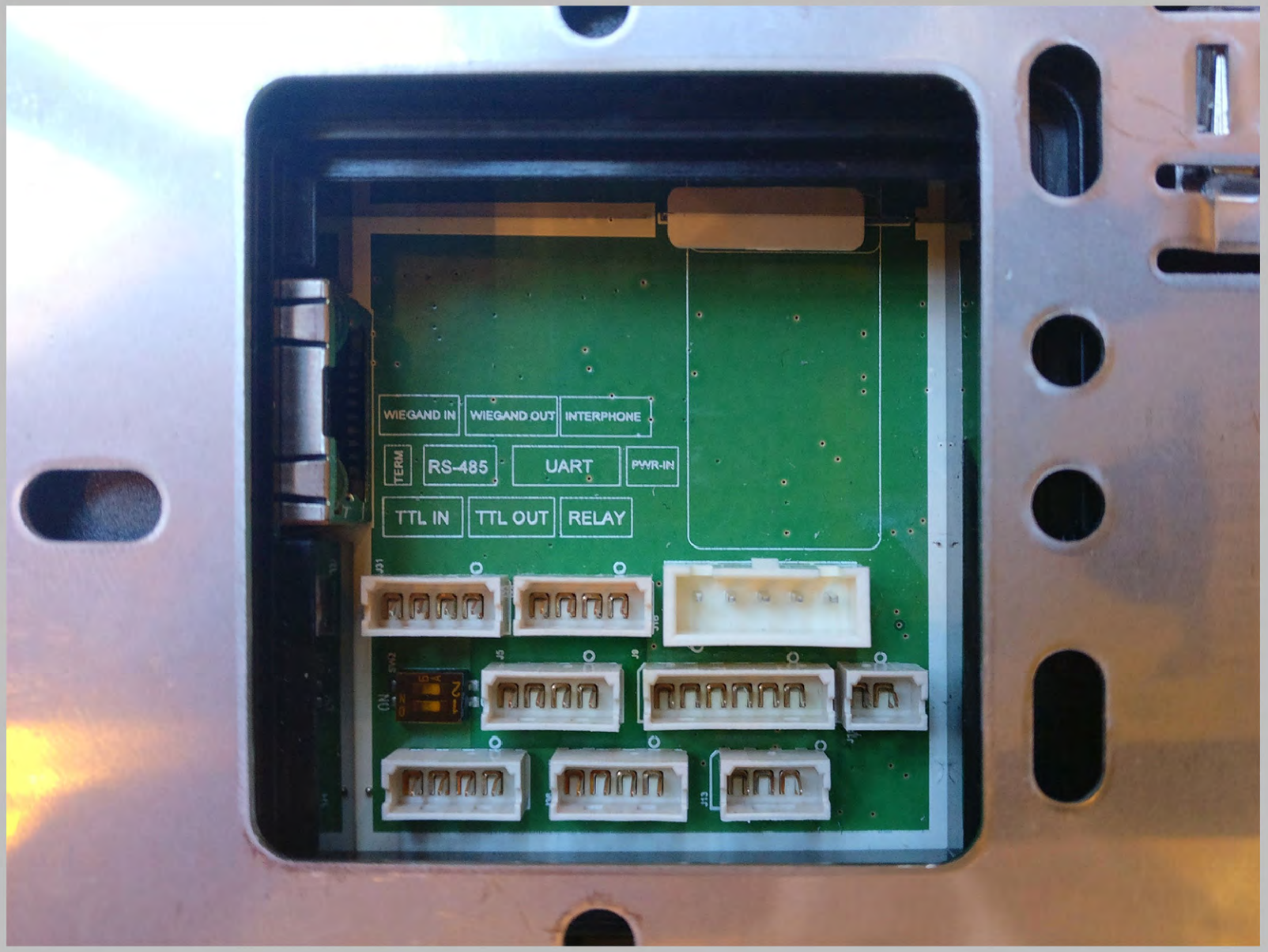
# Real-World Examples



# Real-World Examples



# Real-World Examples



# Real-World Examples



# Real-World Examples



# Remember… The Best Red Teamers



1. Think Unconventionally
2. Attack Across All Surfaces
3. Model the Relevant Threat
4. Demonstrate Impact
5. Interface with the Blue Team

# A Bonus Gift For You All



# Keyed-Alike Systems



# Telephony Access Control Systems



# Many Times the Cabinets are Keyed Alike!



# Keyed-Alike Systems

https://www.gatehousesupplies.com/Linear-key-p/key%20linear.htm

gatehouse
REMOTE CONTROLS & ENTRY SYSTEMS

Parts@gatehousesupplies.com

View Cart | My Account / Order Status | Help | 0 Item

HOME | PRODUCTS | MANUFACTURERS | OUR BRANDS | CONTACT US

Search..

We Will Find You The BEST SHIPPING RATES

Need Help? Contact 866-965-5599

HUGE SALE ON GARAGE DOOR AND GATE EQUIPMENT

Home > Select Products > **Gate Operators & Accessories** > Keypads , Card Readers and Fire Boxes >



A126

## A126 Linear Key

**Availability::** in stock
Product Code: KEY LINEAR

Product Price: **$5.24**

Qty: 1 ADD TO CART

Like 0 Share

View Quantity Discounts

help

### Description

Key for Linear Products

**Features**
Key for Linear Products

# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems

ebay Shop by category | Search... | All Categories | Search | Advanced

Back to home page | Listed in category: Business & Industrial > MRO & Industrial Supply > Safety & Security > Industrial Fire Protection > Fire Alarms

People who viewed this item also viewed


Door King 16120 Double Sided Key
$11.95
Free shipping


Manufacturer Original PK625...
$9.99
Free shipping


Misc. Fire and Security Key Lo...
$21.00
+ $2.25


Misc. Fire and Security Key Lo...
$41.00
+ $2.50




## Door King 16120 Double Sided Key

Item condition: **New**

Quantity: 1 — 3 available / 27 sold

Price: **US $14.95**

Buy It Now

Add to cart

Best Offer: Make Offer

10 watching

Add to watch list

Add to collection

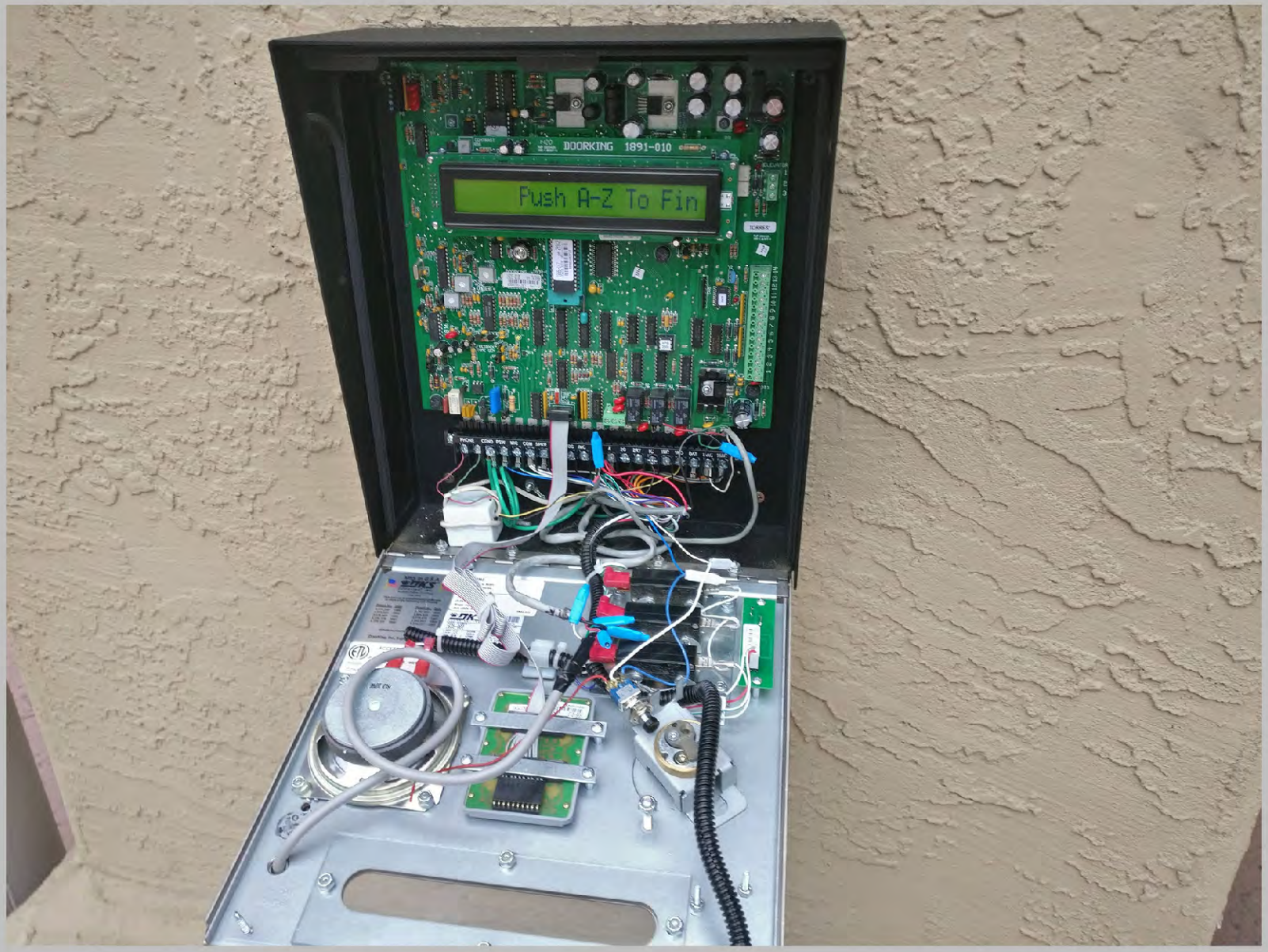
27 sold | More than 89% sold | Free shipping

Add to watch list

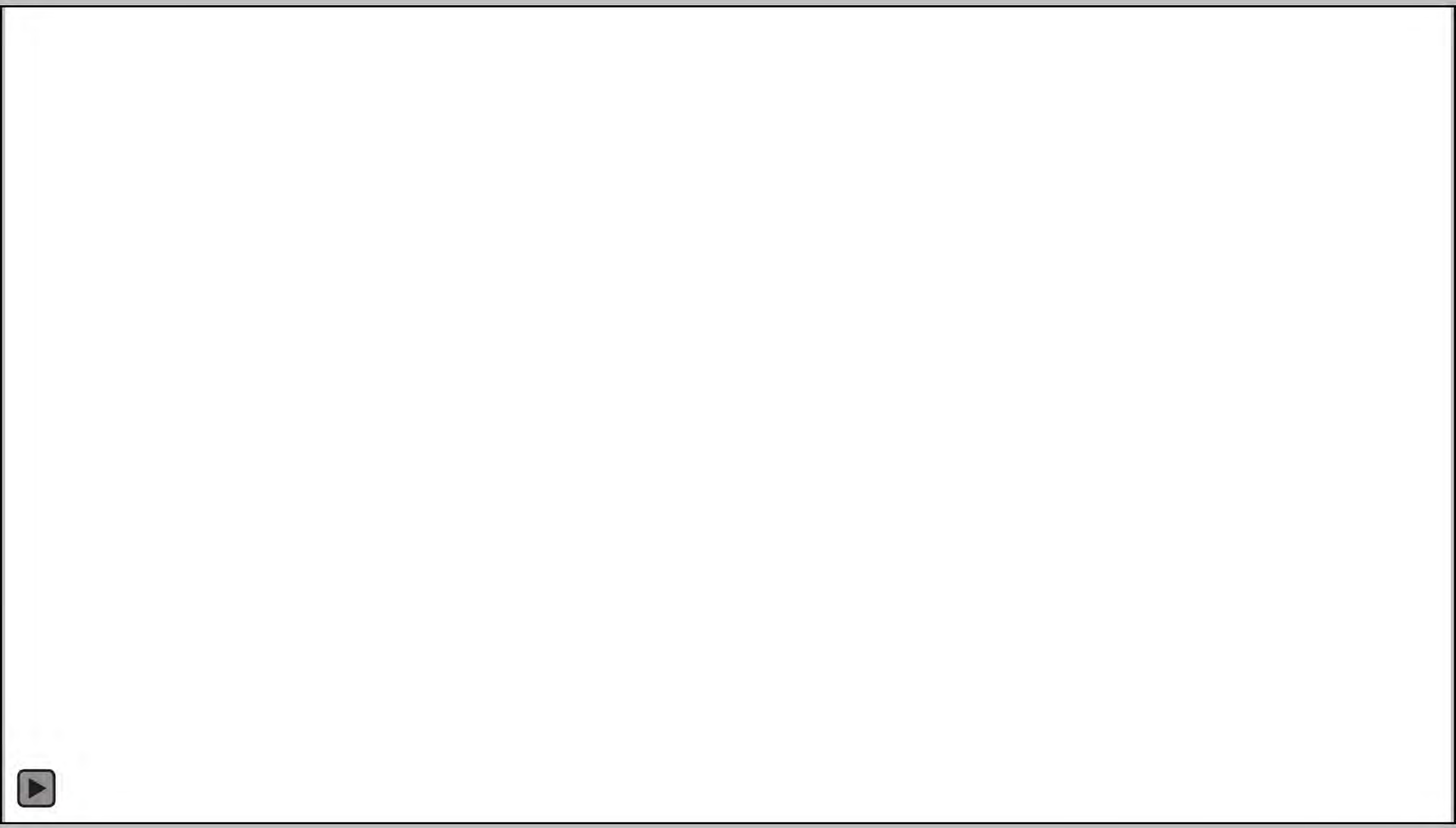
**Seller information**
aghareza2010 (123 ★)
100% Positive feedback

Follow this seller
See other items

# Keyed-Alike Systems



# Keyed-Alike Systems



# Other Keyed-Alike Tips



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



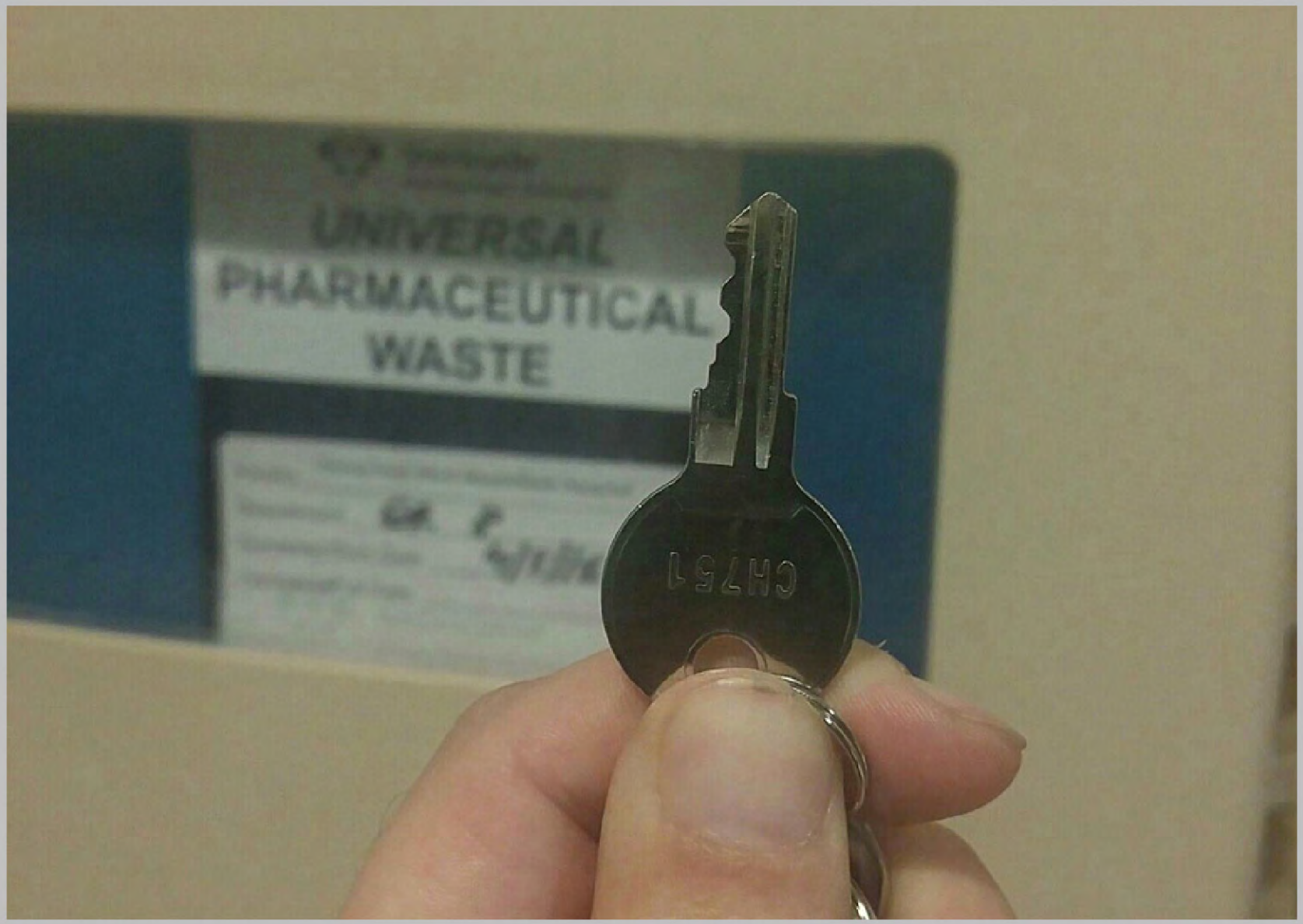
# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems

https://www.amazon.com/CH751-Key-OEM-keys-pack/dp/B001562UII

amazon Try Prime | Tools & Home Improvement | Departments | Your Amazon.com | Today's Deals | Gift Cards & Registry | Sell | Help | Hello. Sign in Your Account | Try Prime | Lists | 0 Cart

Tools & Home Improvement | Best Sellers | Gift Ideas | Lighting & Ceiling Fans | Hardware | Kitchen & Bath Fixtures | Power & Hand Tools | Woodworking | Home Automation

School Lists — Teachers, make your supply lists easy — Learn more

What do customers buy after viewing this item?

**Best Selling**



Southco
**This item:** CH751 Key OEM (10 keys per pack)
10
$8.79 Prime

**Top Rated**



Others
1 X REPLACEMENT KEY FOR PYRAMID PTR 4000, 4000HD, 3500, & 3700 TIME CLOCK
6
$6.81 Prime

**Lowest Price**



Hunter and Rainbird
Hunter and Rainbird Sprinkler Controller Door Key
48
$5.15

Office Products › Office & School Supplies › Forms, Recordkeeping & Money Handling › Key Tags & Chains





## CH751 Key OEM (10 keys per pack)

by Southco
10 customer reviews

Price: $8.79 & **FREE Shipping** on orders over $49. Details

Only 16 left in stock.
**Want it Tuesday, July 5?** Order within **28 hrs 42 mins** and choose **Two-Day Shipping** at checkout. Details
Sold by OCSParts and Fulfilled by Amazon. Gift-wrap available.

- CH751 Key OEM (10 keys per pack)

› See more product details

Share

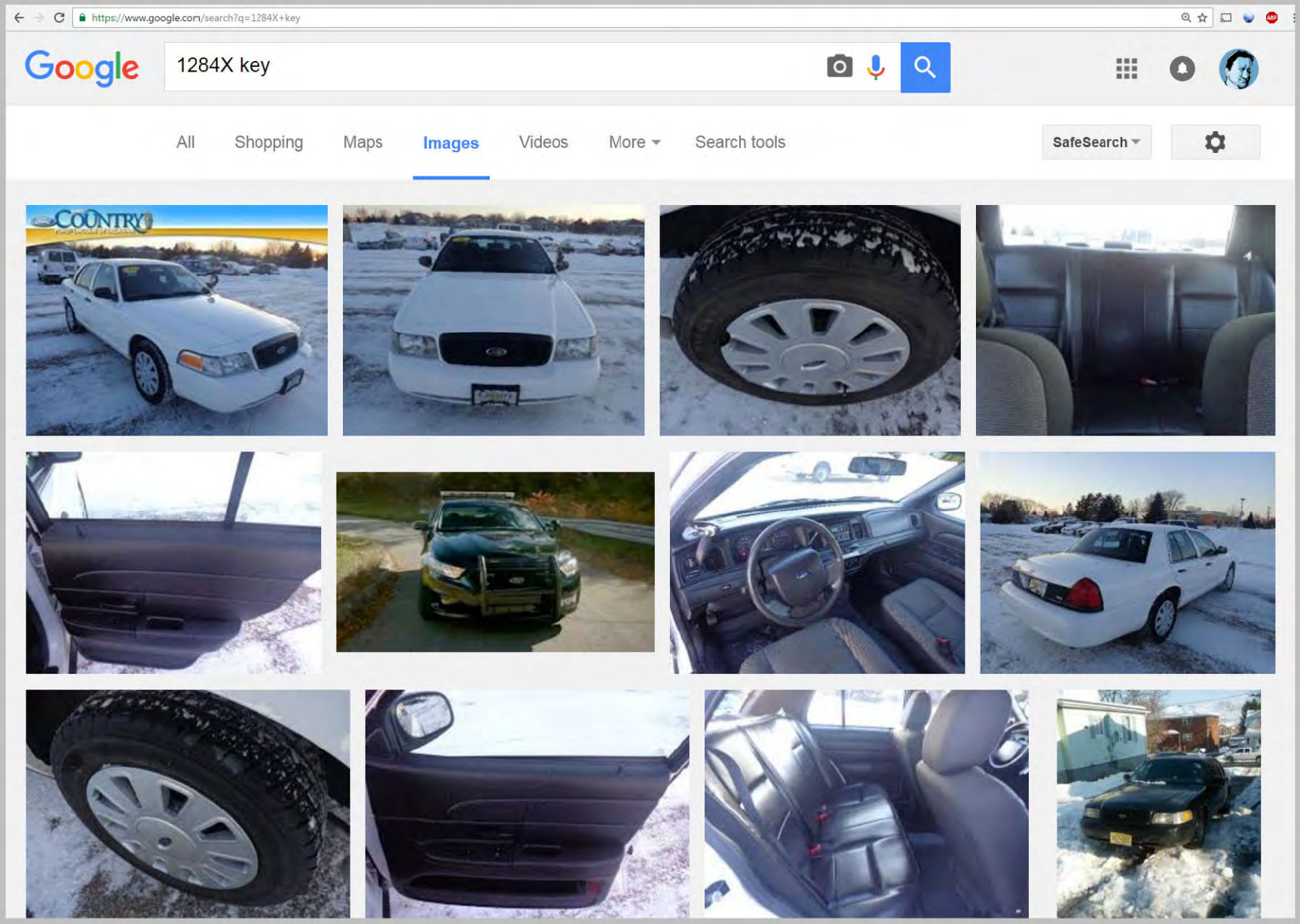
Qty: 1

Yes, I want **FREE Two-Day Shipping** with Amazon Prime

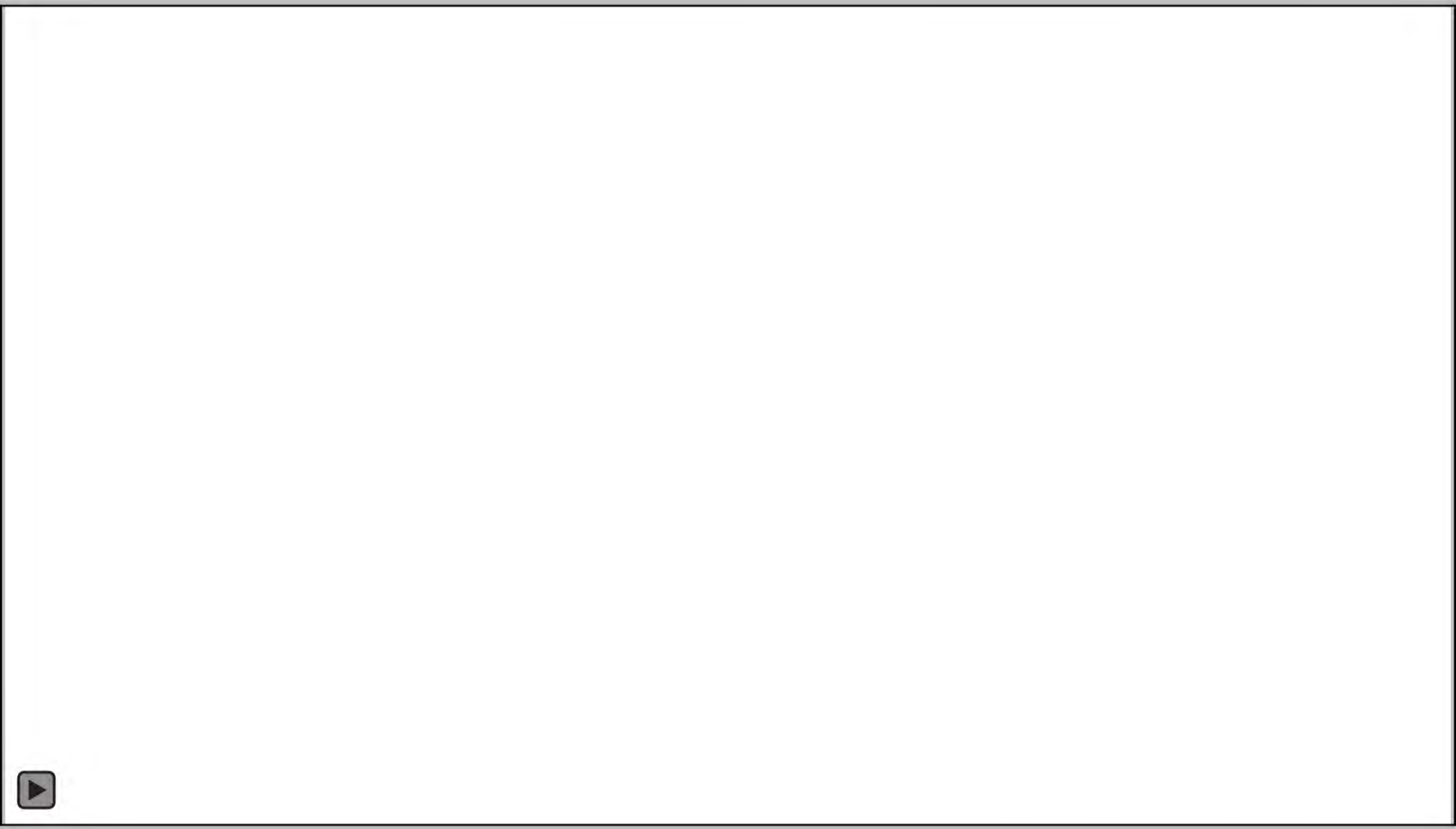
Add to Cart

Turn on 1-Click ordering for this browser

# Keyed-Alike Systems



# Keyed-Alike Systems



# Keyed-Alike Systems



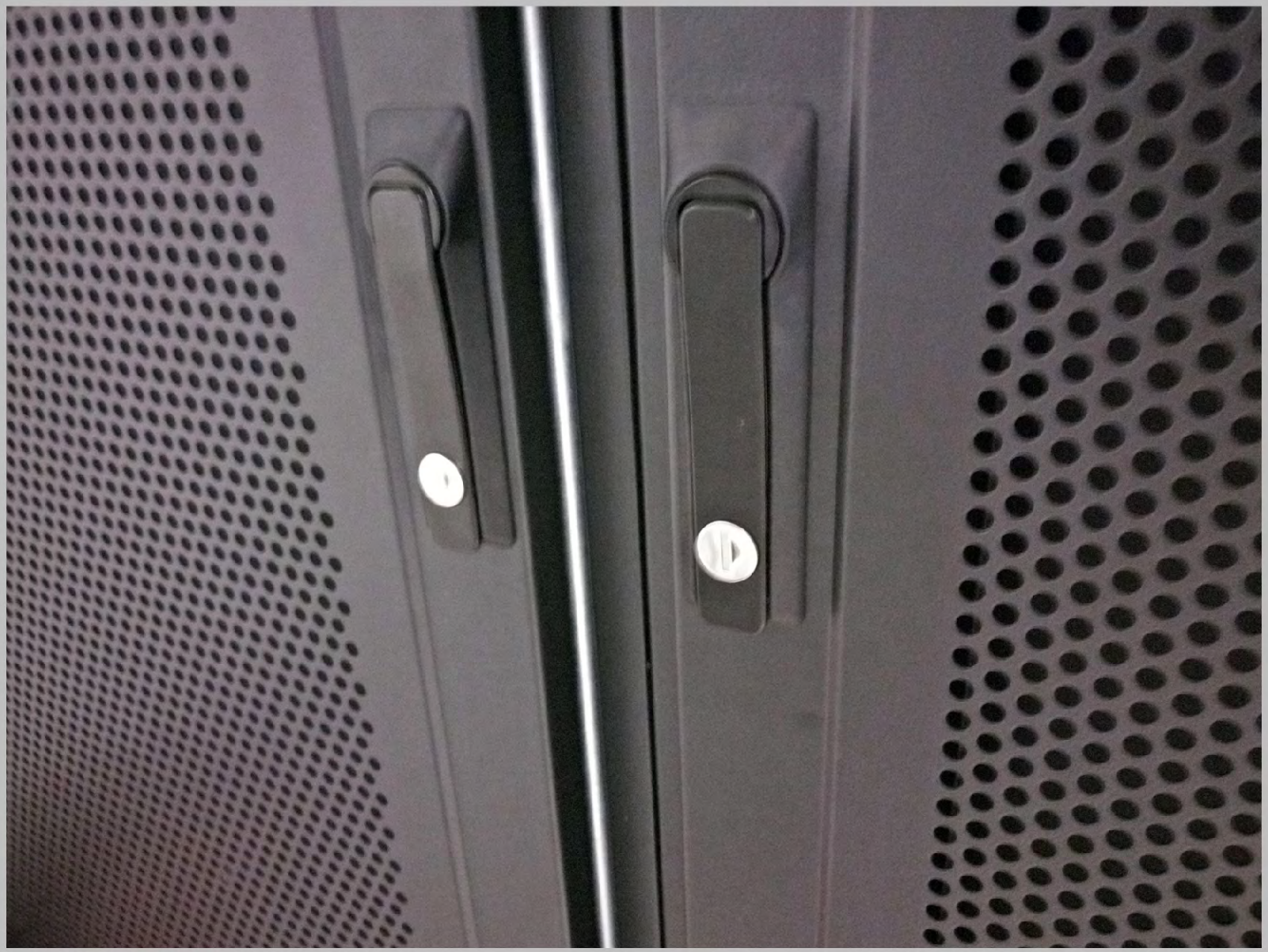
# Keyed-Alike Systems



# EMKA Industrial Keys



# EMKA Industrial Keys



# EMKA Industrial Keys



# EMKA Industrial Keys









# Dev's Previous Everyday Carry Keyring



# Dev’s New Everyday Carry Set

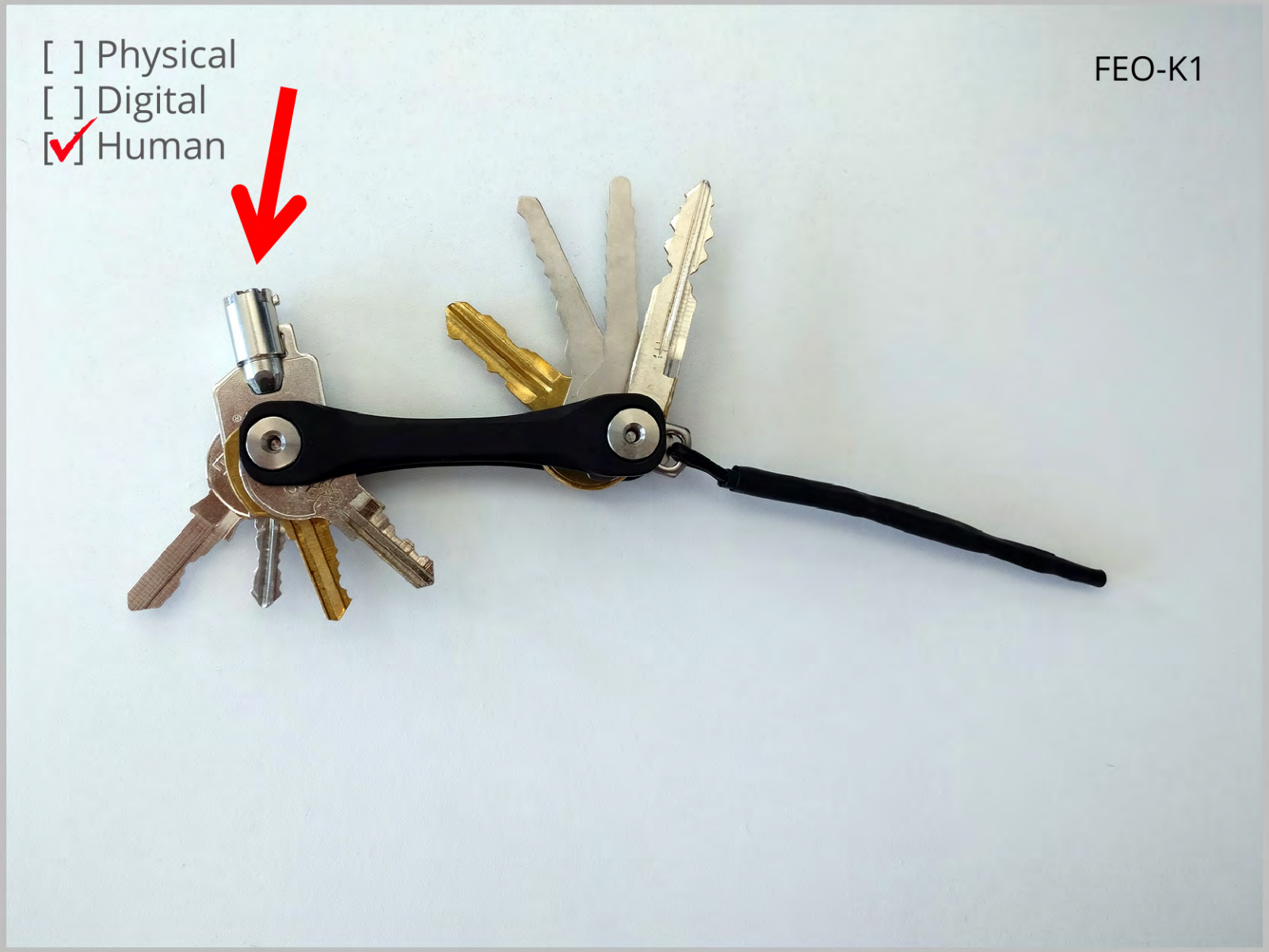


# Dev's New Everyday Carry Set

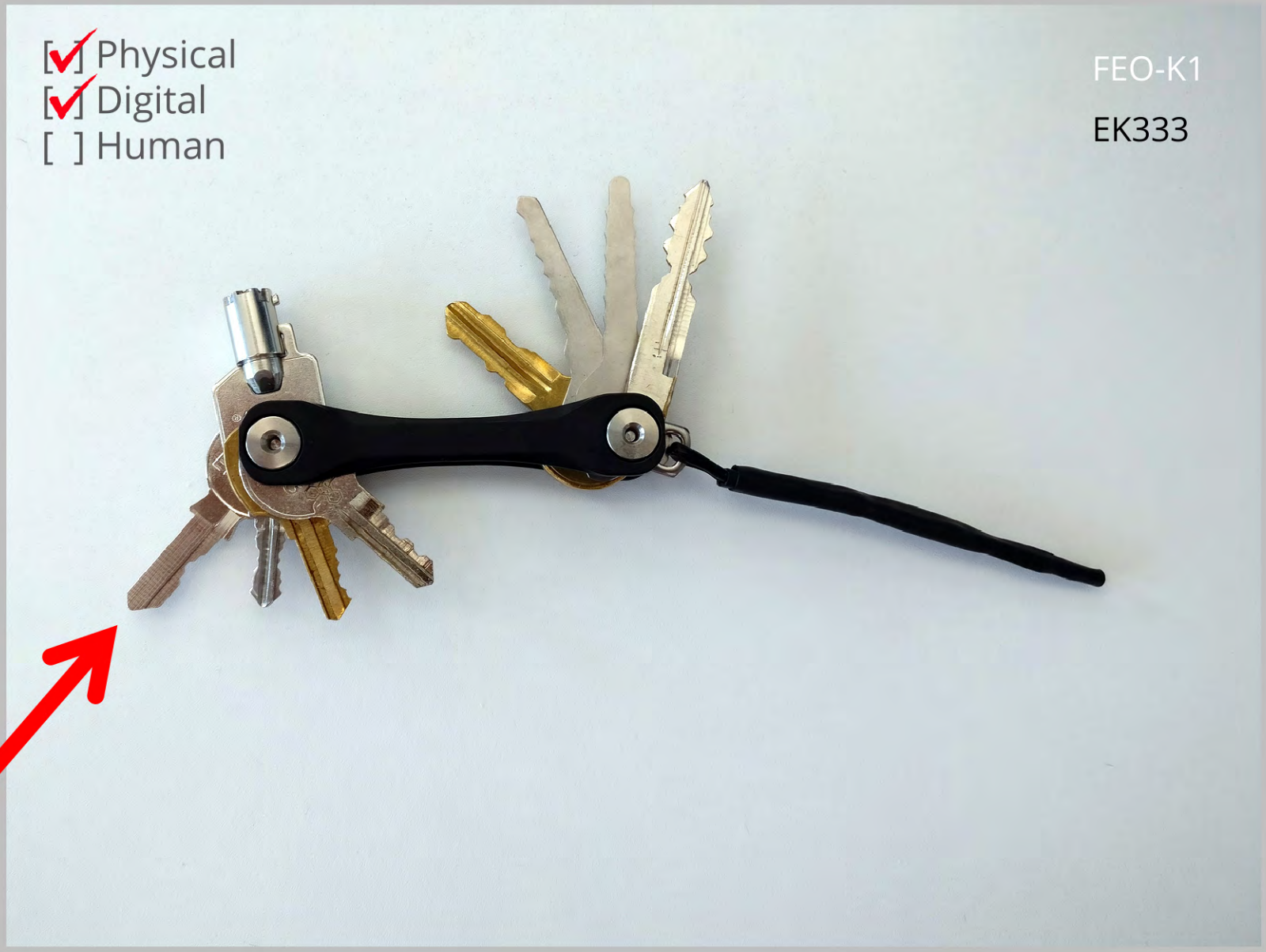
[ ] Physical
[ ] Digital
[ ] Human



# Dev's New Everyday Carry Set



# Dev's New Everyday Carry Set



# Dev's New Everyday Carry Set

[x] Physical
[x] Digital
[ ] Human

FEO-K1

EK333

222343



# Dev's New Everyday Carry Set

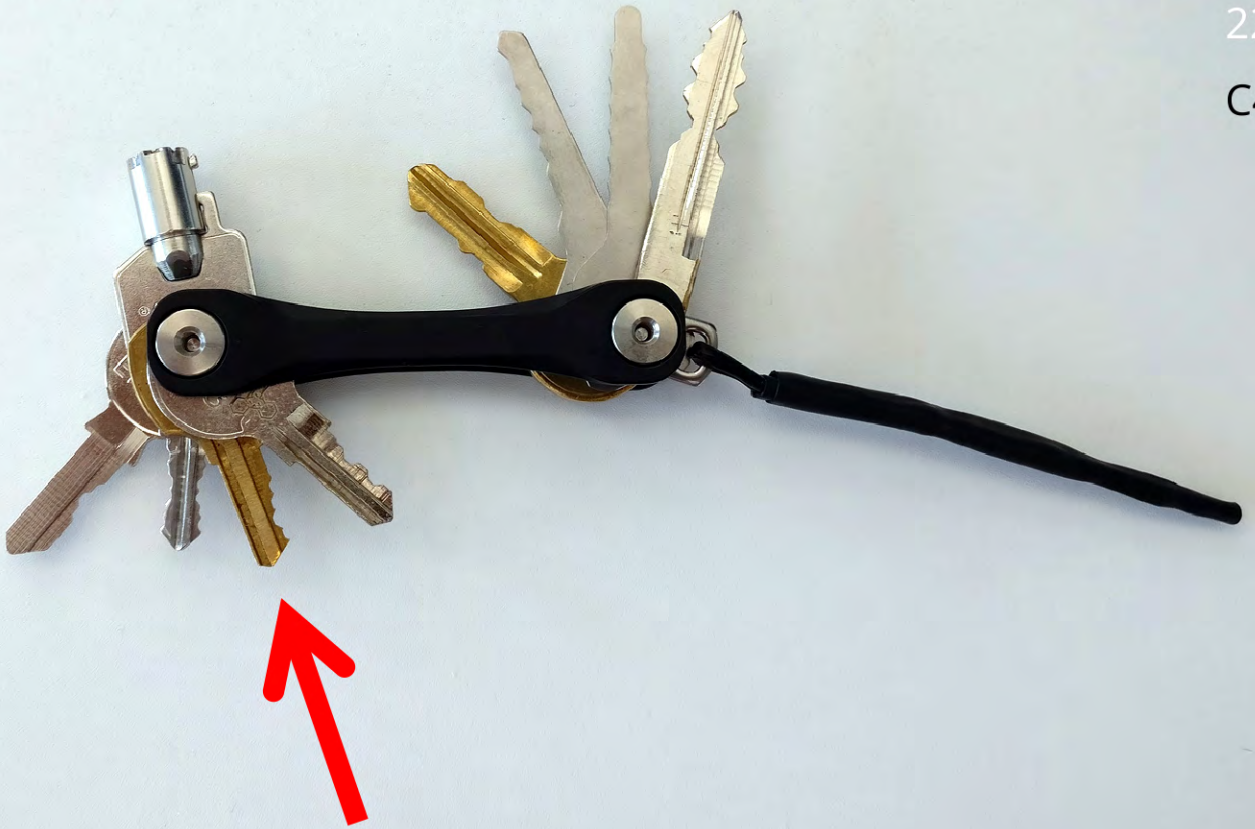
[✓] Physical
[ ] Digital
[ ] Human

FEO-K1

EK333

222343

C415A



# Dev's New Everyday Carry Set

[✓] Physical
[ ] Digital
[ ] Human



FEO-K1

EK333

222343

C415A

CH751

# Dev's New Everyday Carry Set

[x] Physical
[x] Digital
[ ] Human



FEO-K1

EK333

222343

C415A

CH751

16120

# Dev's New Everyday Carry Set

[✓] Physical
[ ] Digital
[ ] Human



FEO-K1

EK333

222343

C415A

CH751

16120

Jigglers

# Dev's New Everyday Carry Set

[ ] Physical
[ ] Digital
[✓] Human



FEO-K1

EK333

222343

C415A

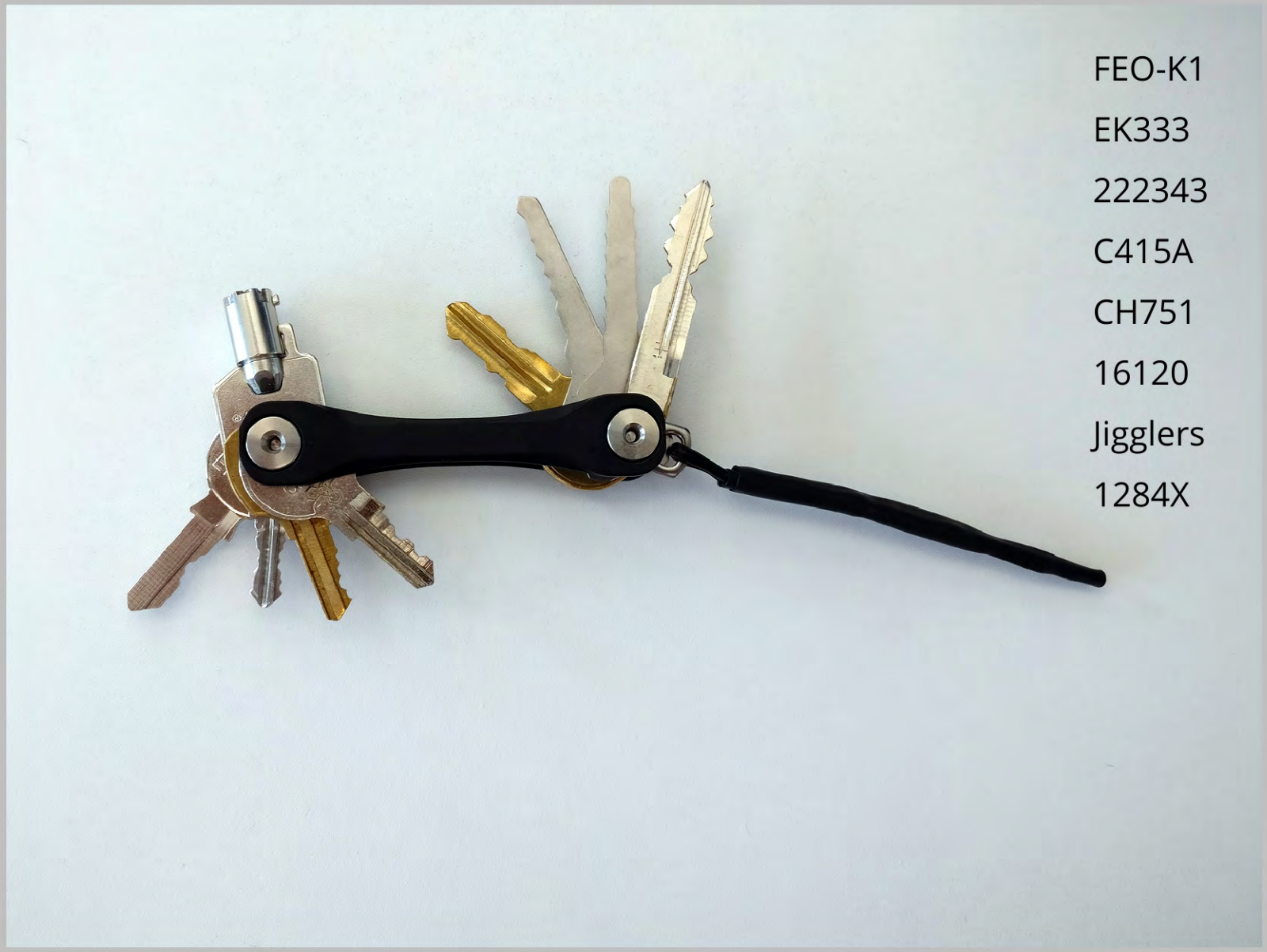
CH751

16120

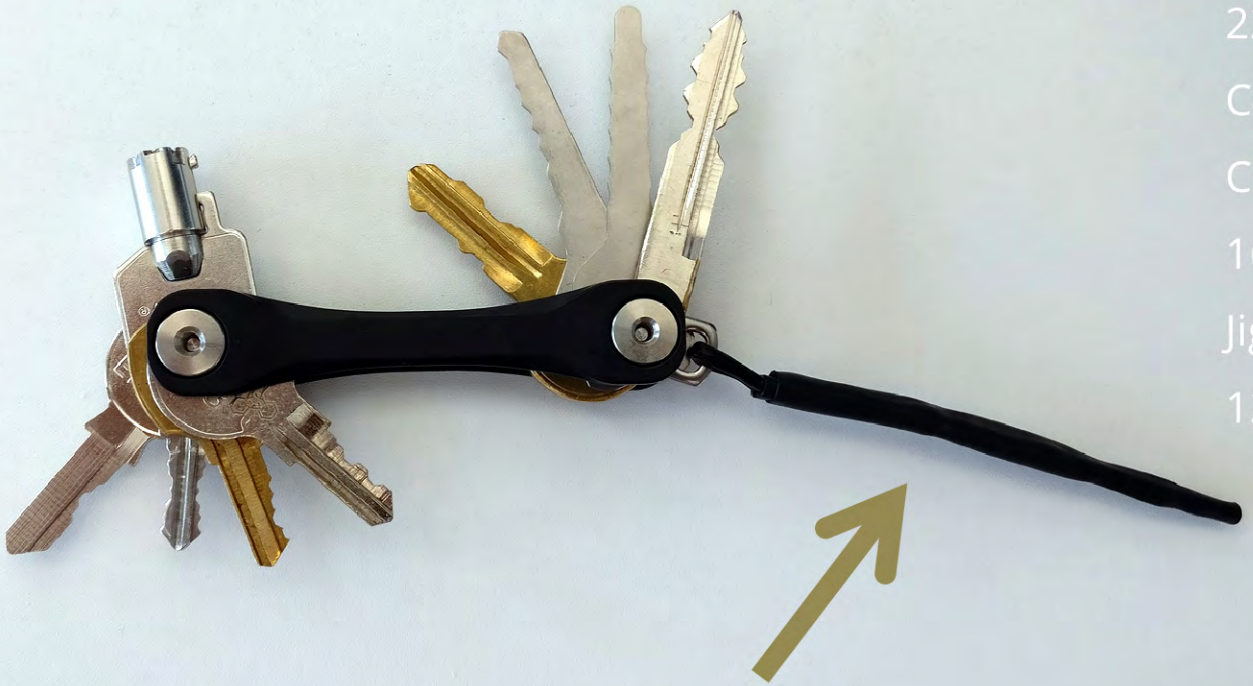
Jigglers

1284X

# Dev’s New Everyday Carry Set



# Dev's New Everyday Carry Set



FEO-K1

EK333

222343

C415A

CH751

16120

Jigglers

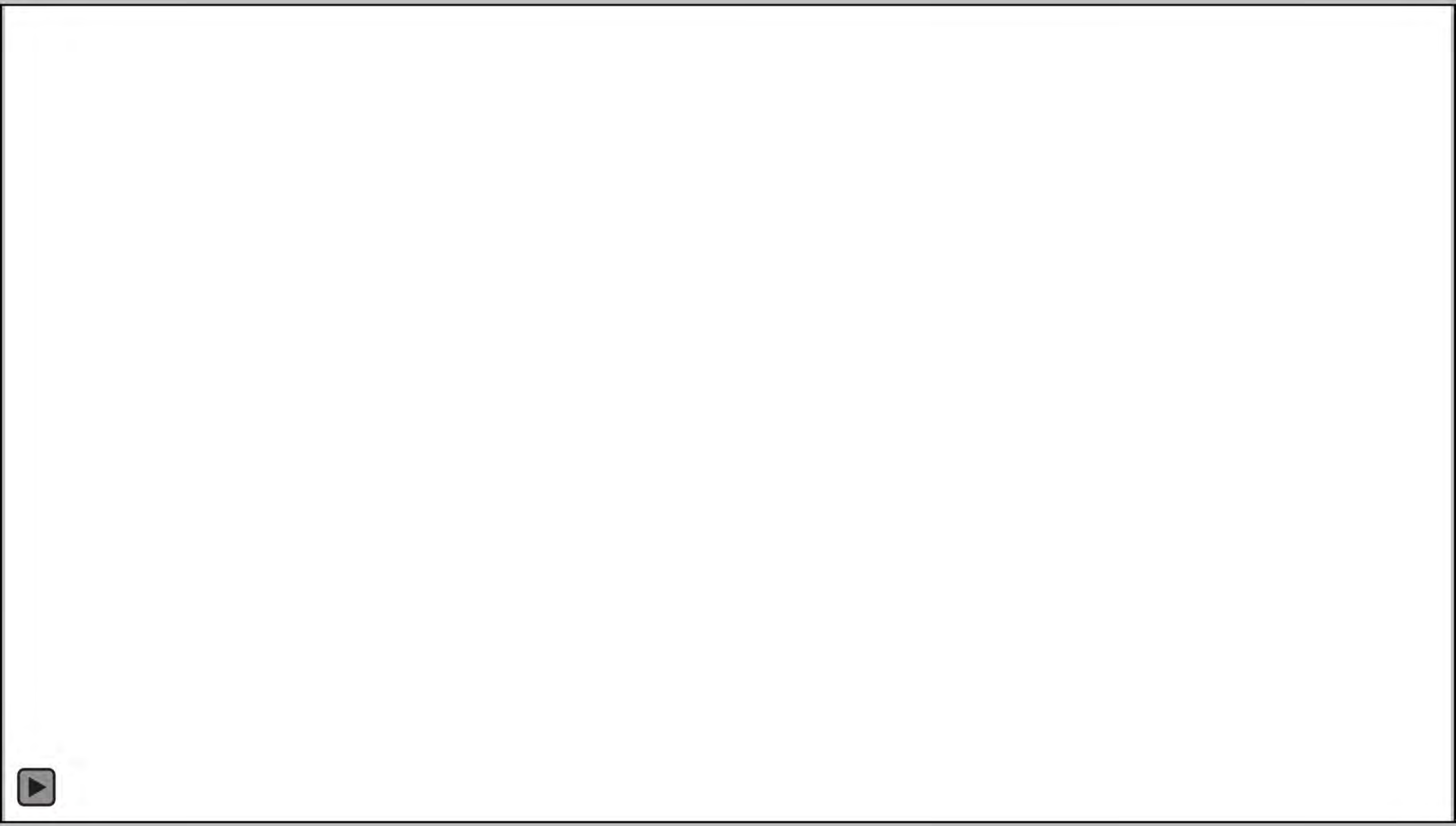
1284X

then what's this?

# Dev's New Everyday Carry Set



# Dev's New Everyday Carry Set



# Dev's New Everyday Carry Set



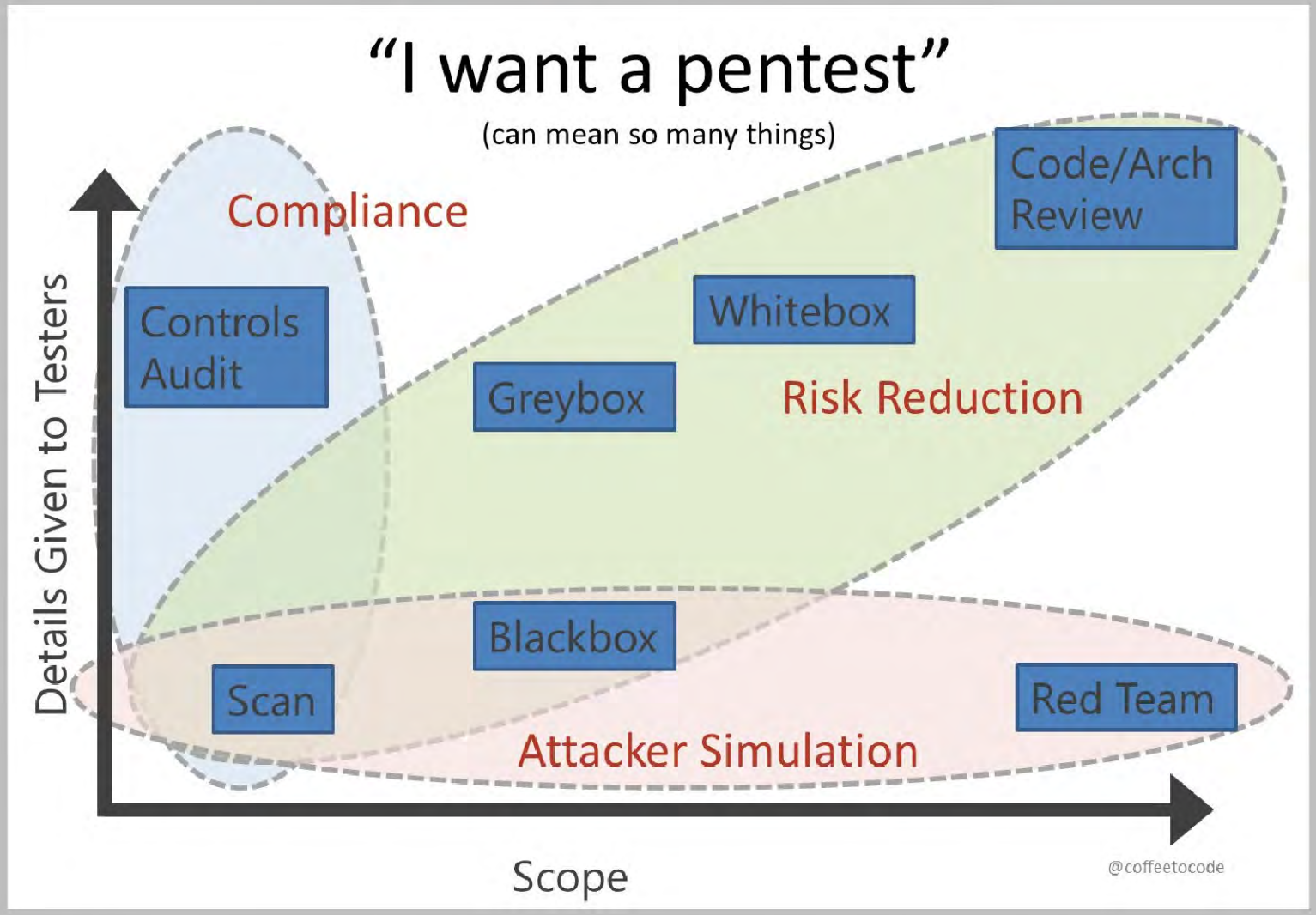
# Dev's New Everyday Carry Set



# In Conclusion



# Untangling the Terminology




https://twitter.com/coffeetocode/status/794593057282859008

# “On Pentesting, Professionalism, & Chill”

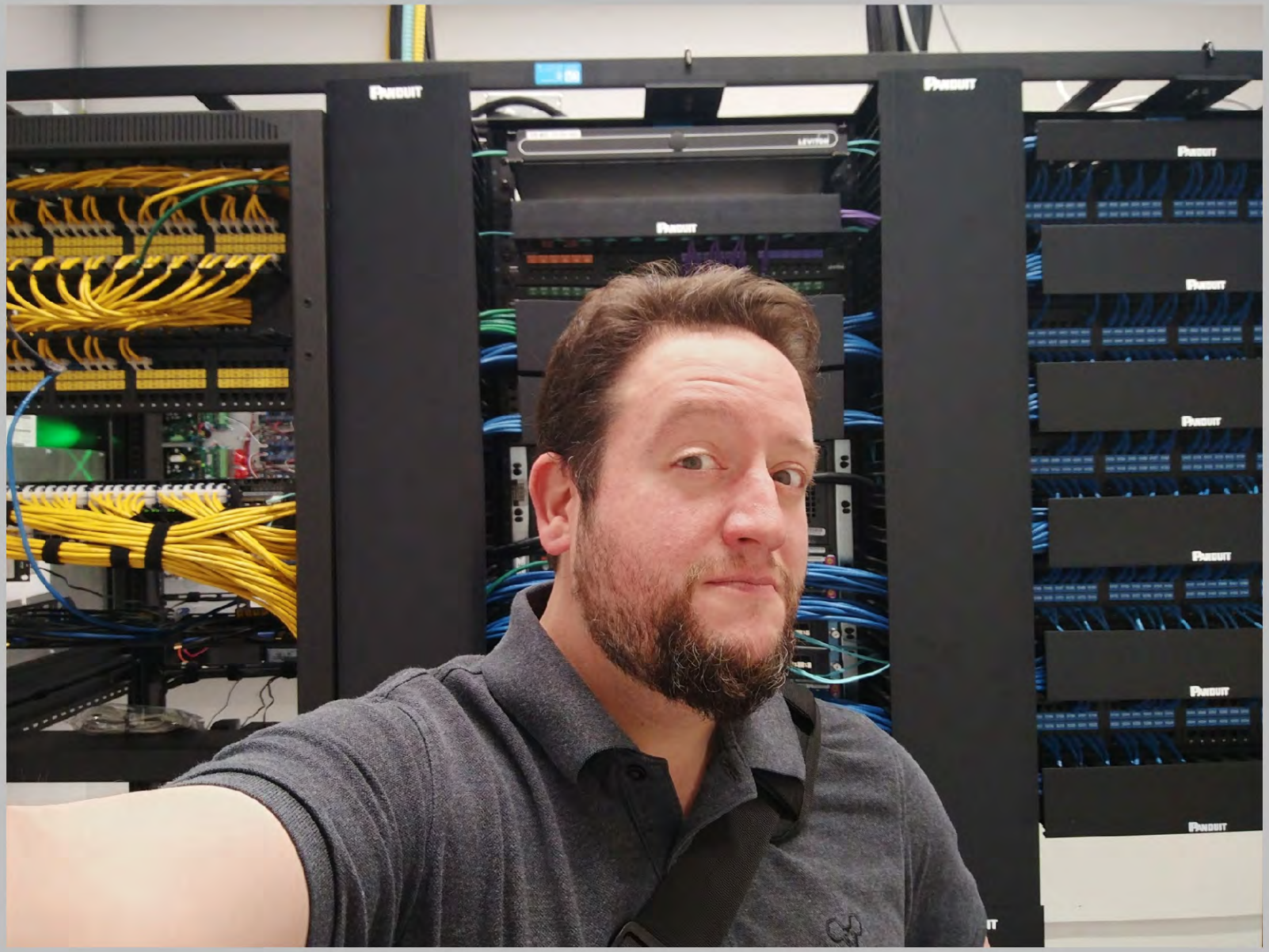


https://coffeetocode.net/2016/09/on-pentesting-professionalism-chill

# Work Together to be Better Together



# Getting in is Fun... Getting Caught is the Goal



# Let’s Keep Making Things Better



# *Thank You Very Much*

delta@enterthecore.net
at the office

@deviantollam
on twitter

"whiskey, neat"
at the bar

