Subverting Physical Access Controls

Tactics of Physical Pen Testers

Deviant Ollam

Swiss Cyber Storm – 2017/10/18

Who Am I?

Security Consultant By Day

Criminal Consultant By Night

Basically… I'm Professionally Dangerous

Why Does Physical Security Matter ?

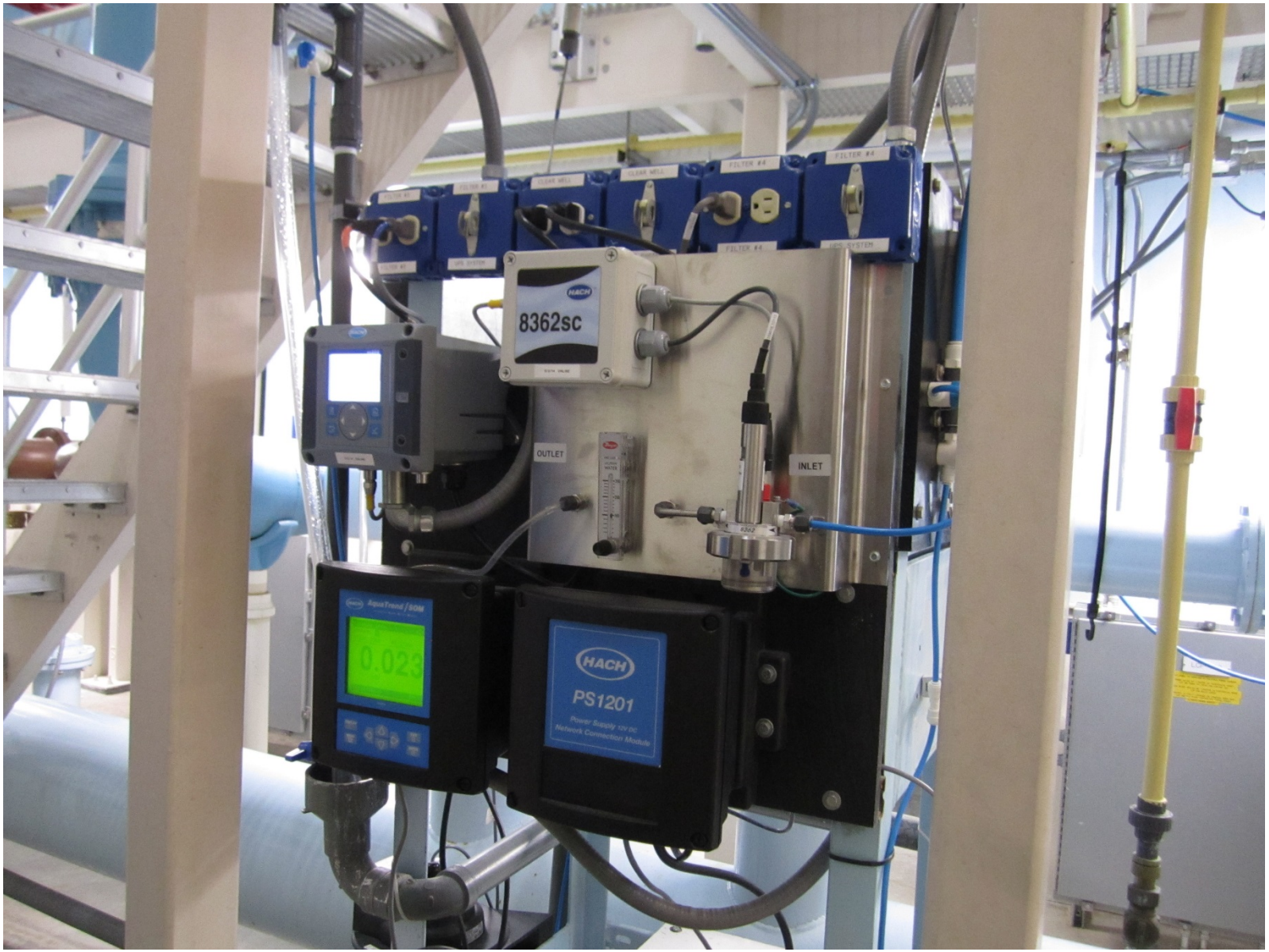
All of your firewall rules...

All of your firewall rules... can be compromised

All your hard work here...

All your hard work here... gets undermined here

Hands-On Attacks are Possible On-Site



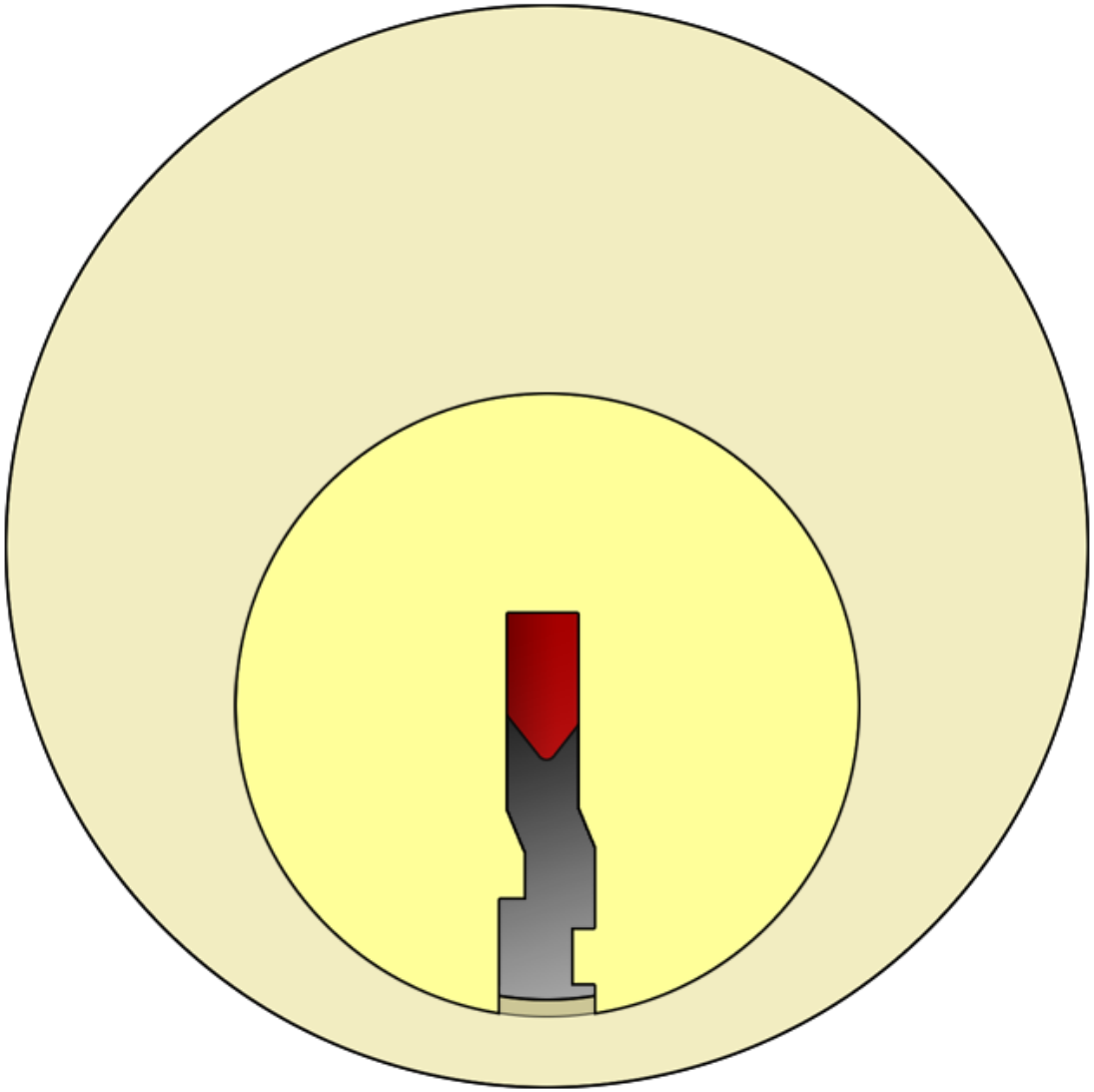
Who's Tried Lockpicking?

We All Use Locks

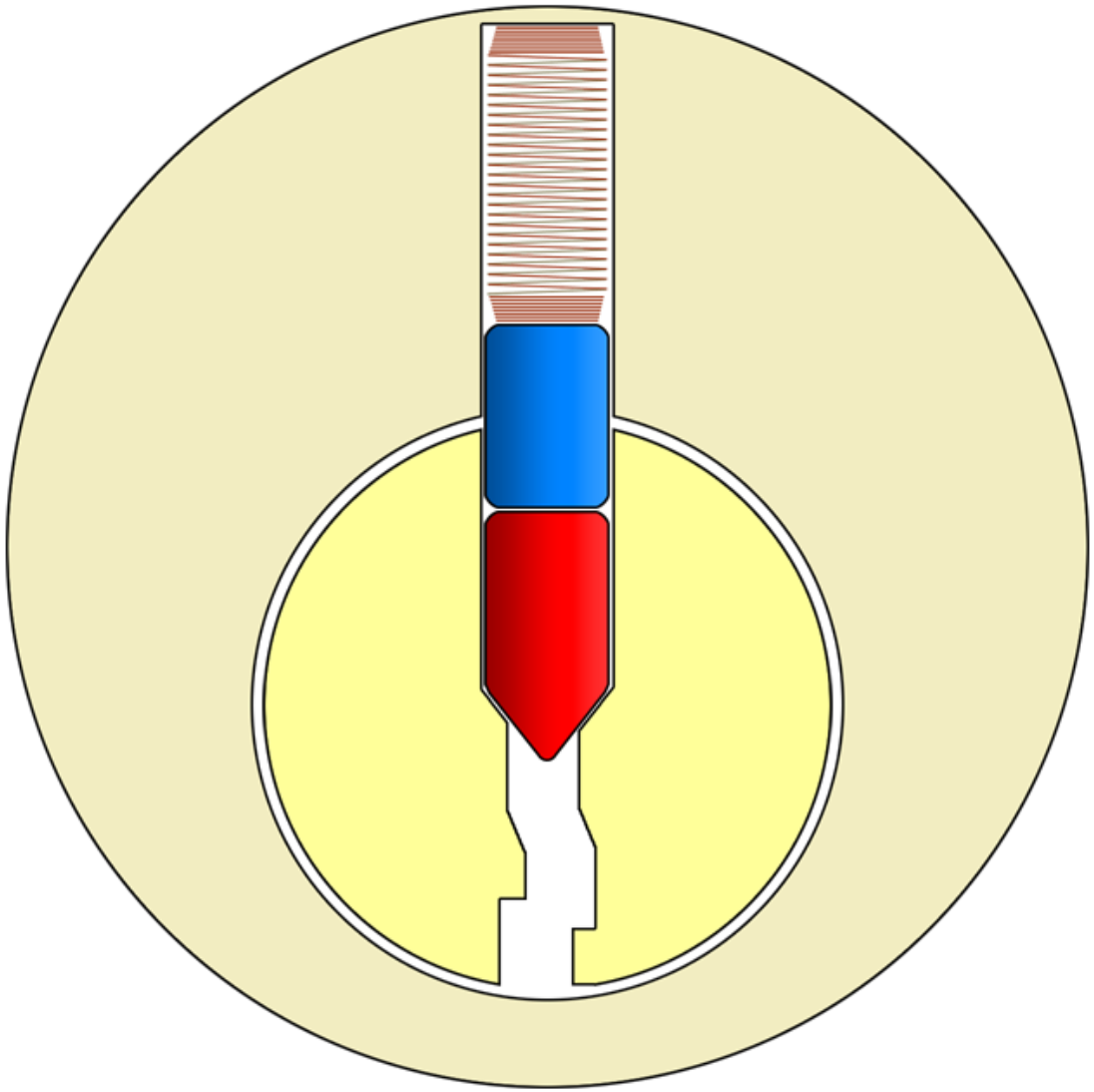
We All Use Locks

We All Use Locks

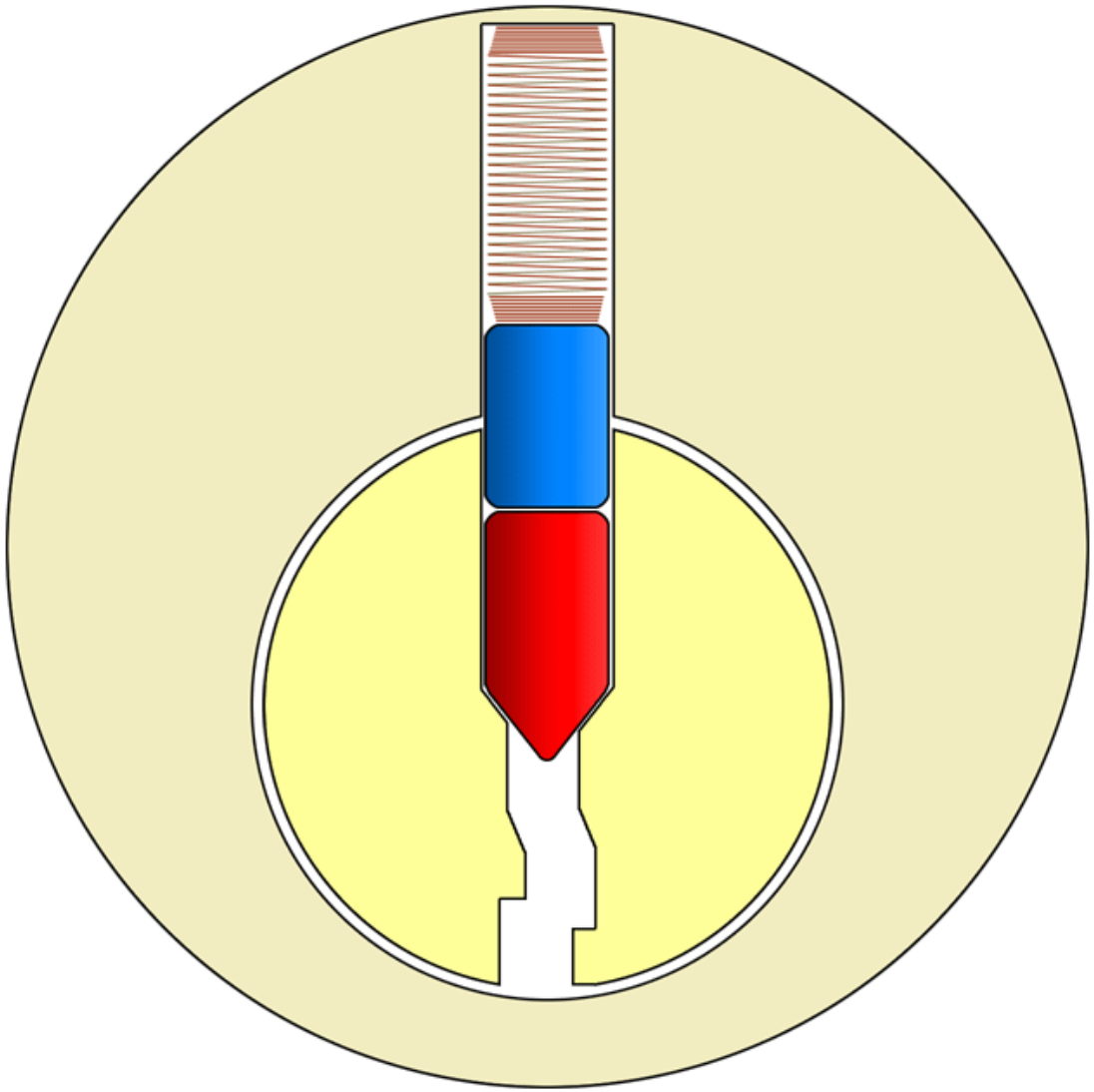
Outer View



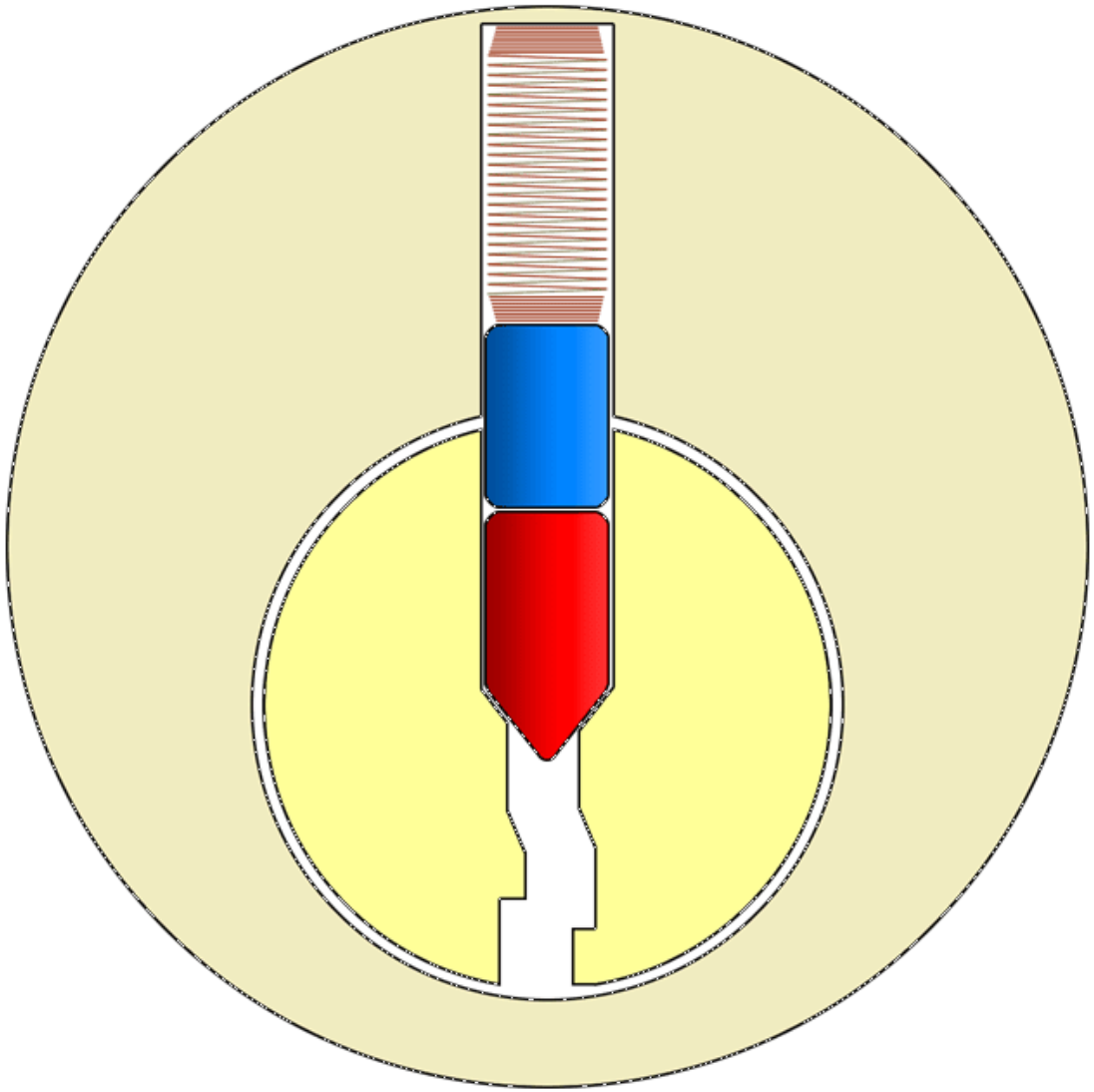
Inner View



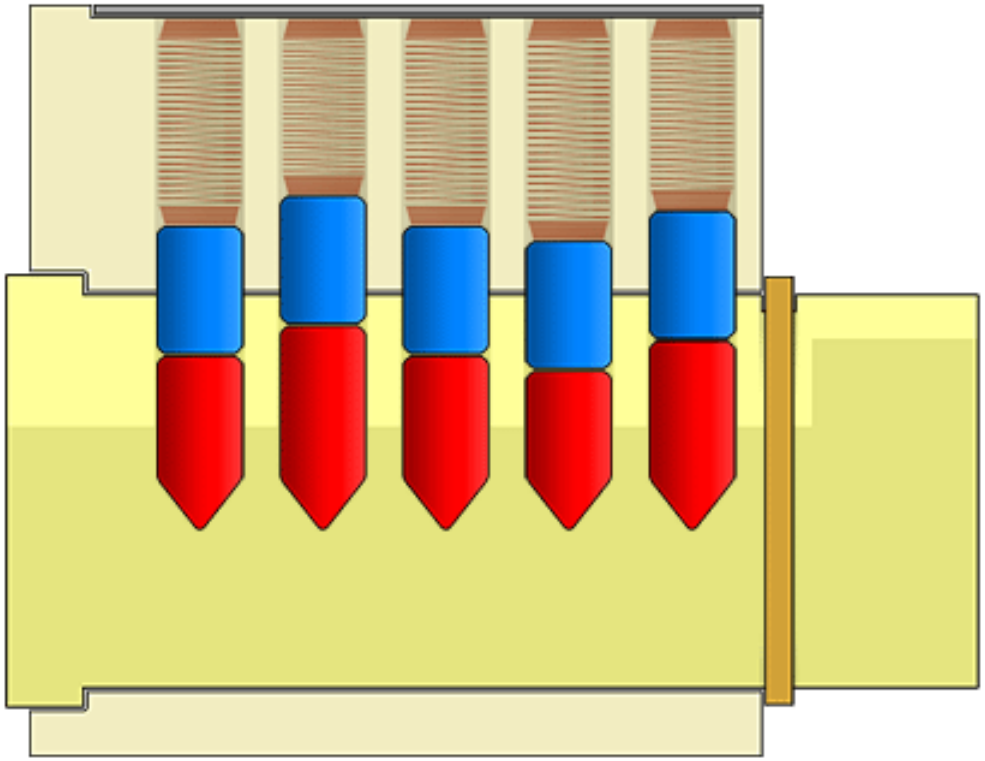
Attempt Without a Key



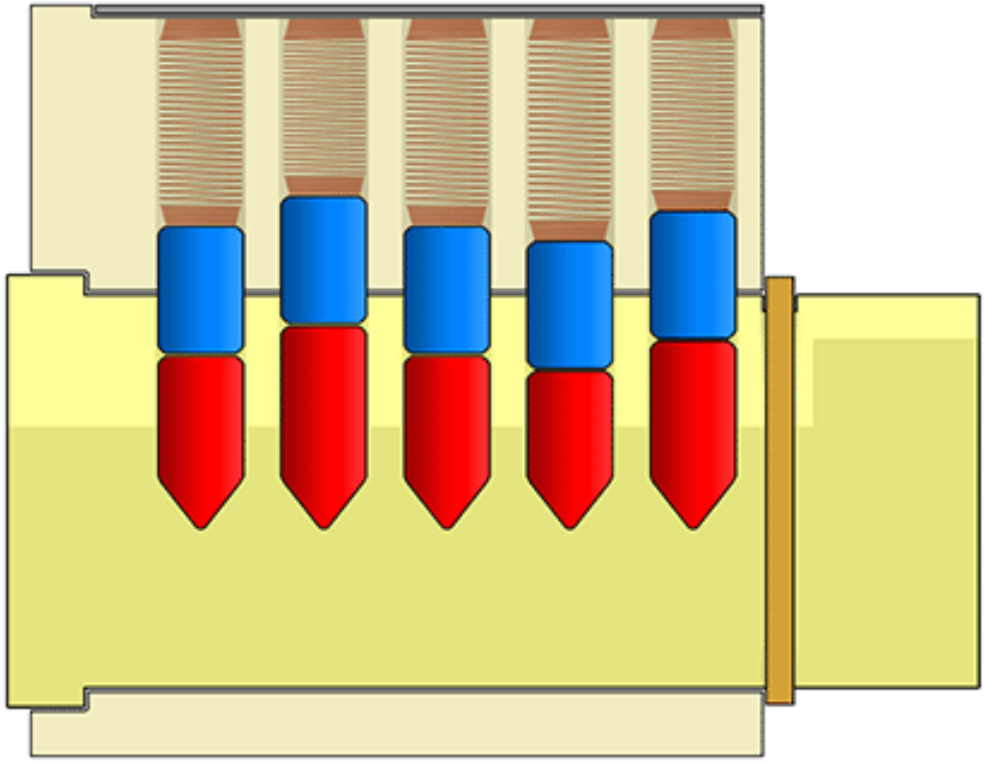
Opening With a Key



Opening With a Key



Opening *Without* a Key



But Why Pick When You Can Bypass?

Door Latch Attacks

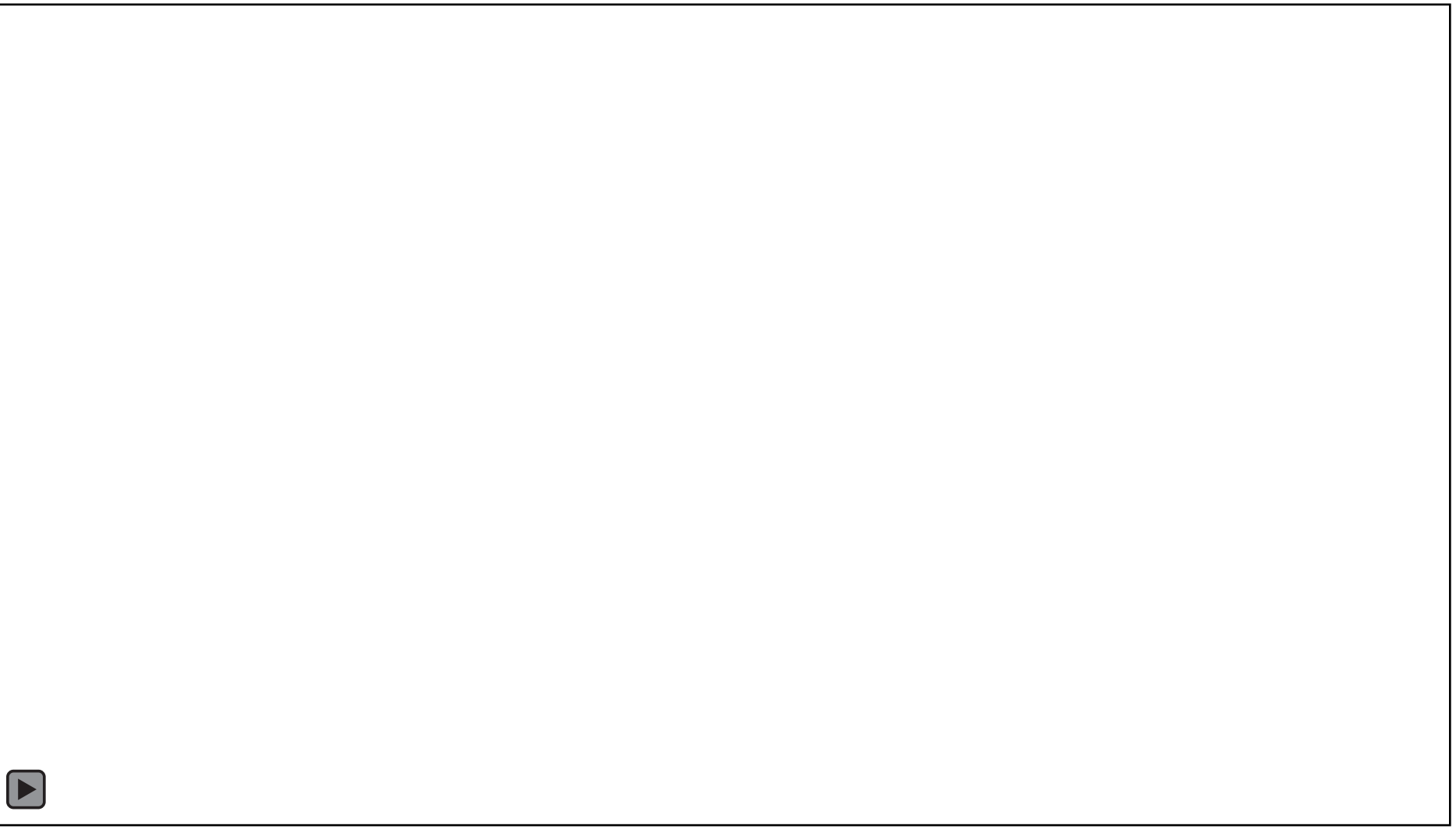
Shrum Tools / Traveler Hooks

Shrum Tools / Traveler Hooks

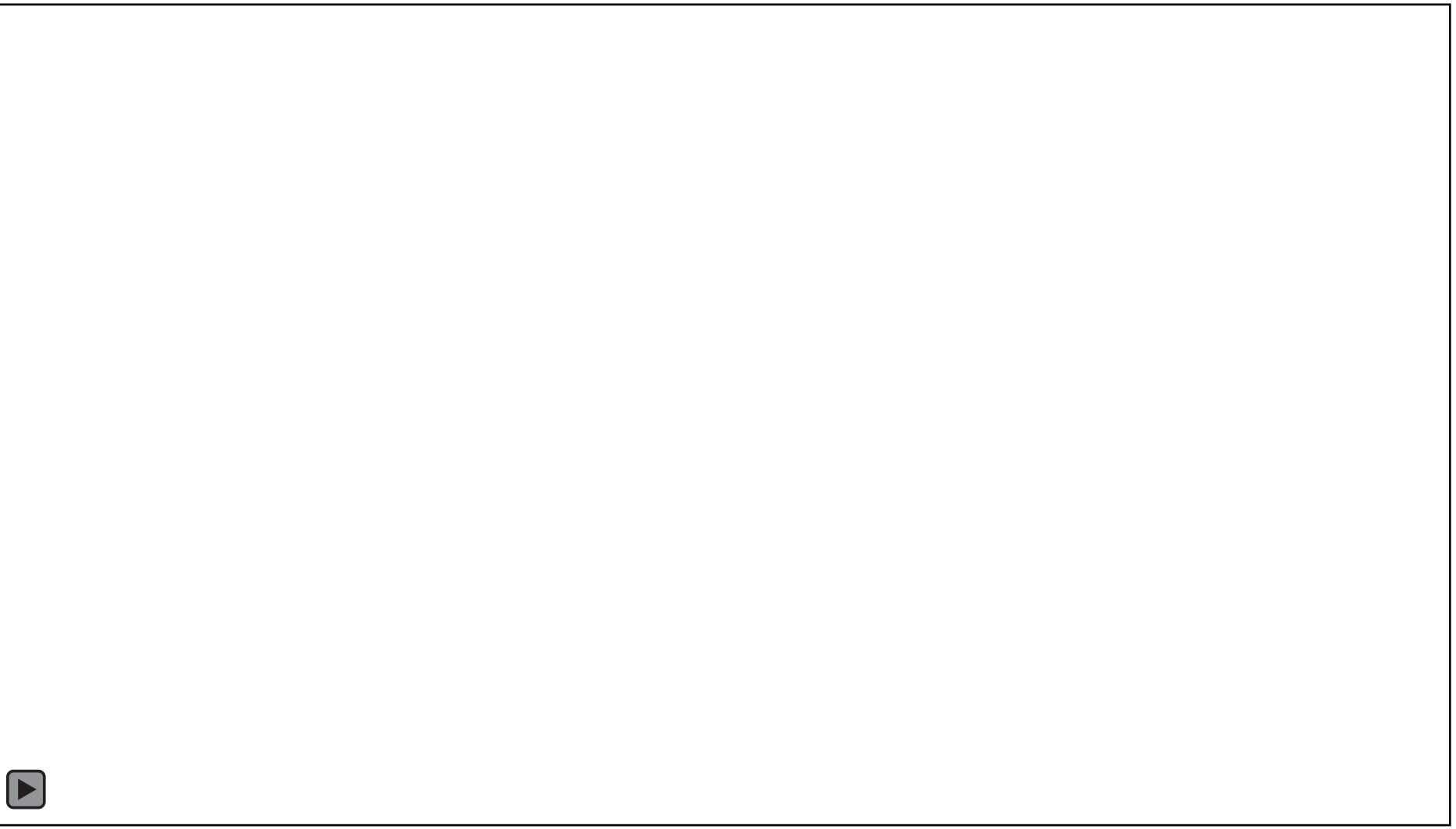
Shrum Tools / Traveler Hooks

Shrum Tools / Traveler Hooks

Door Bypassing

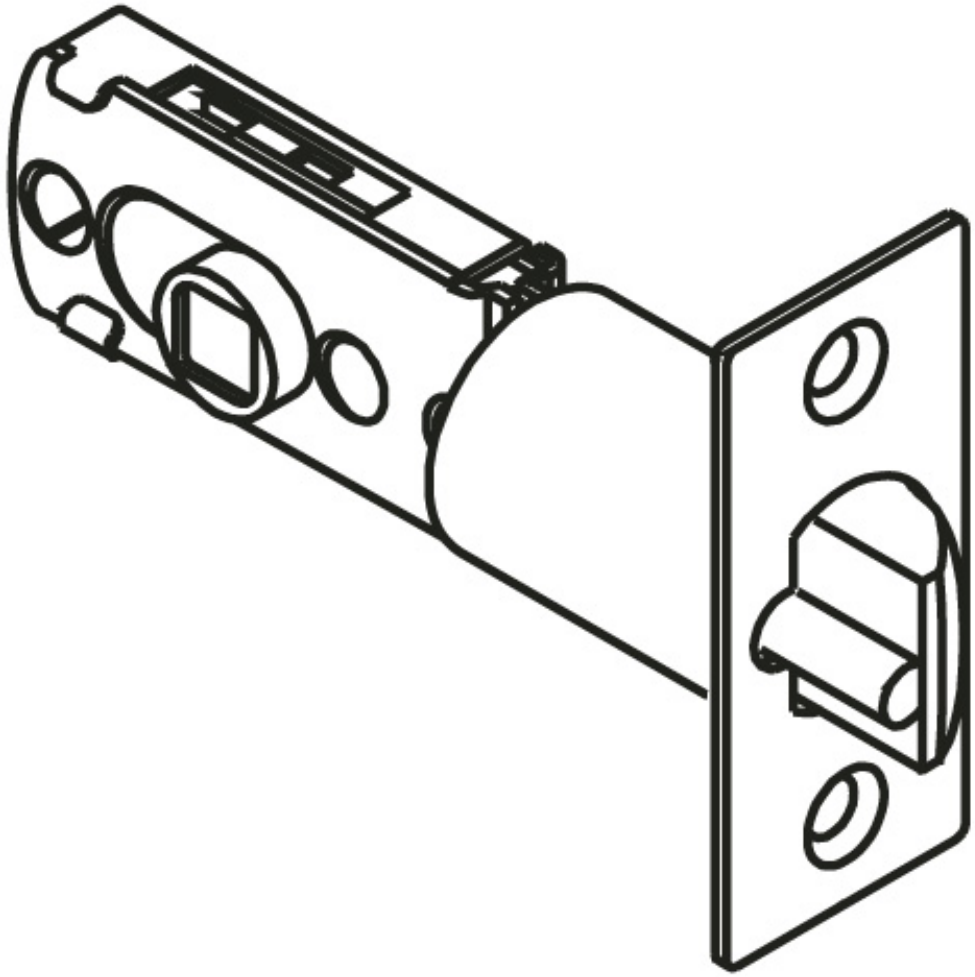


Door Bypassing

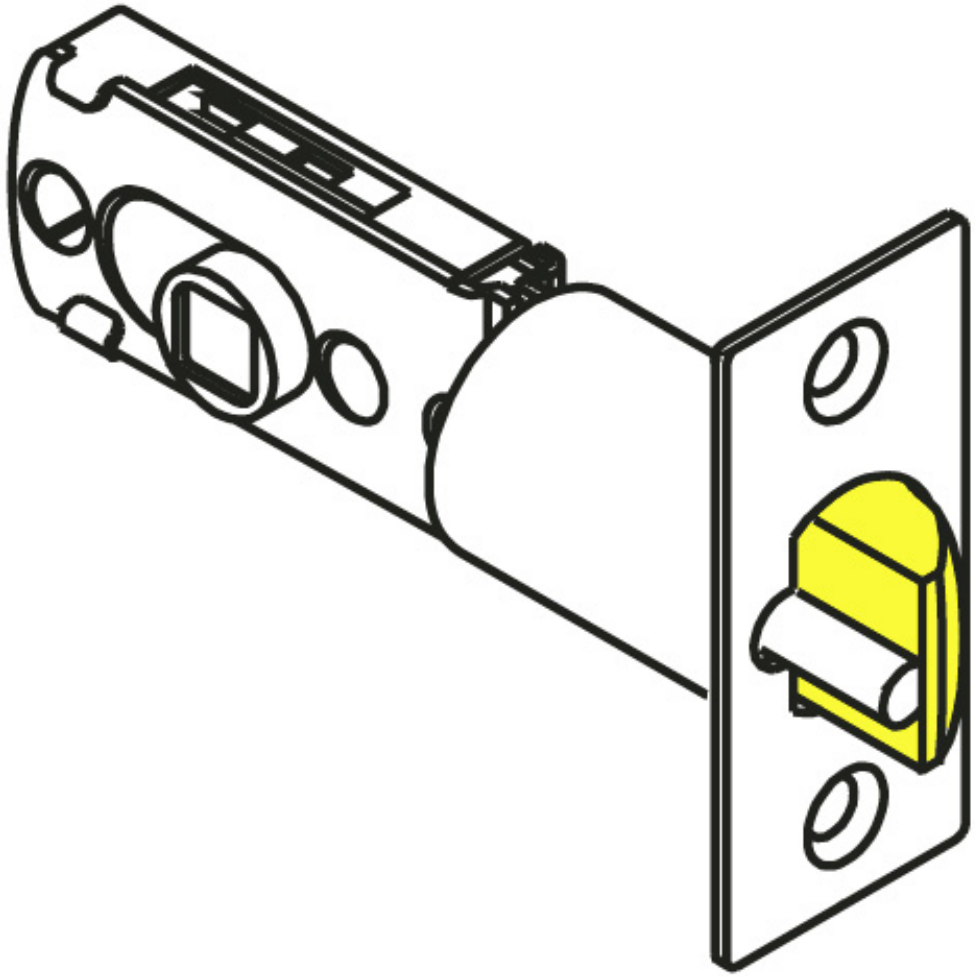


Protective Plates?

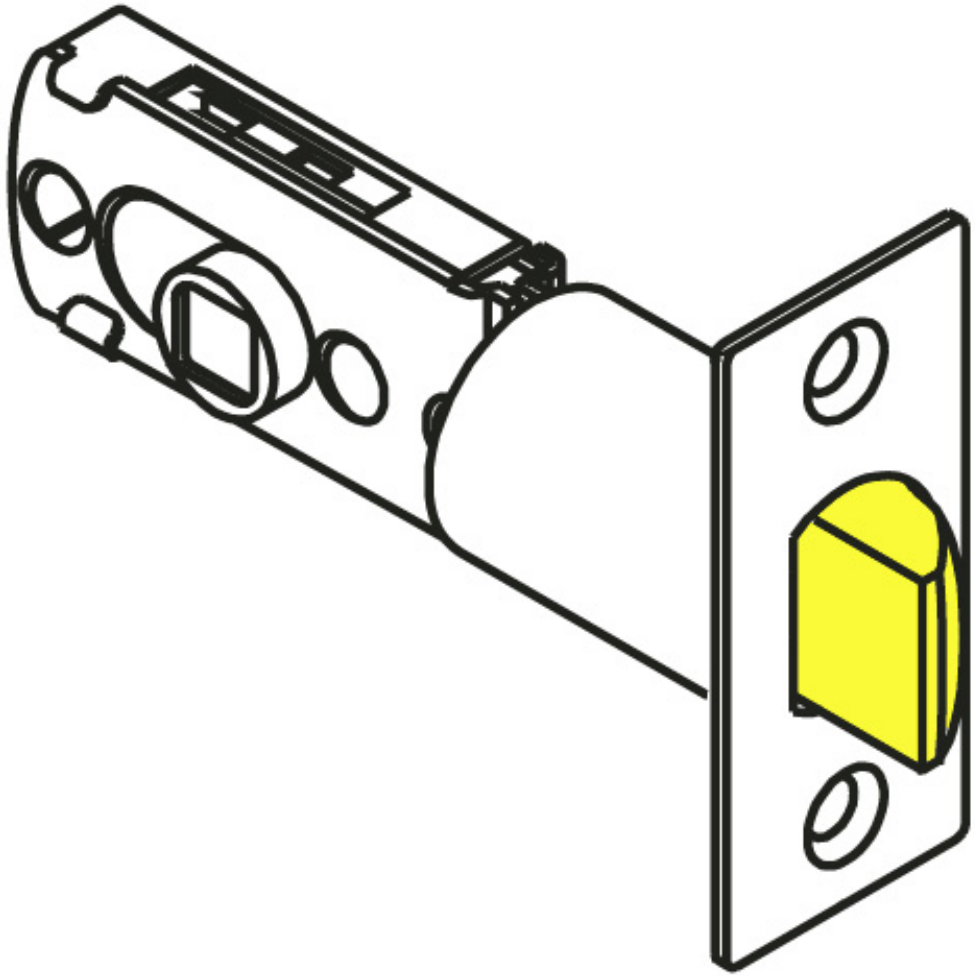
Dead Latches



Dead Latches

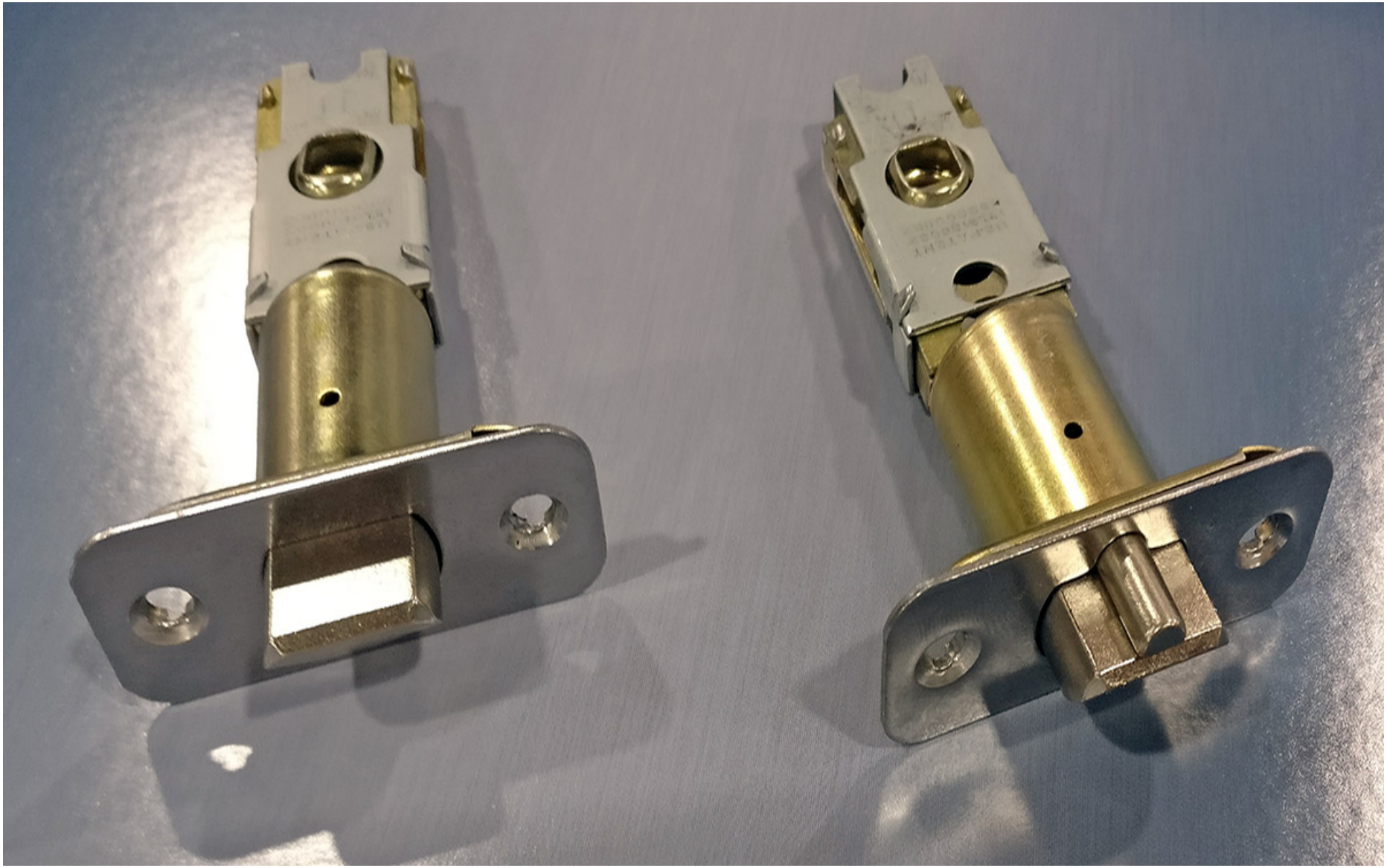


Dead Latches

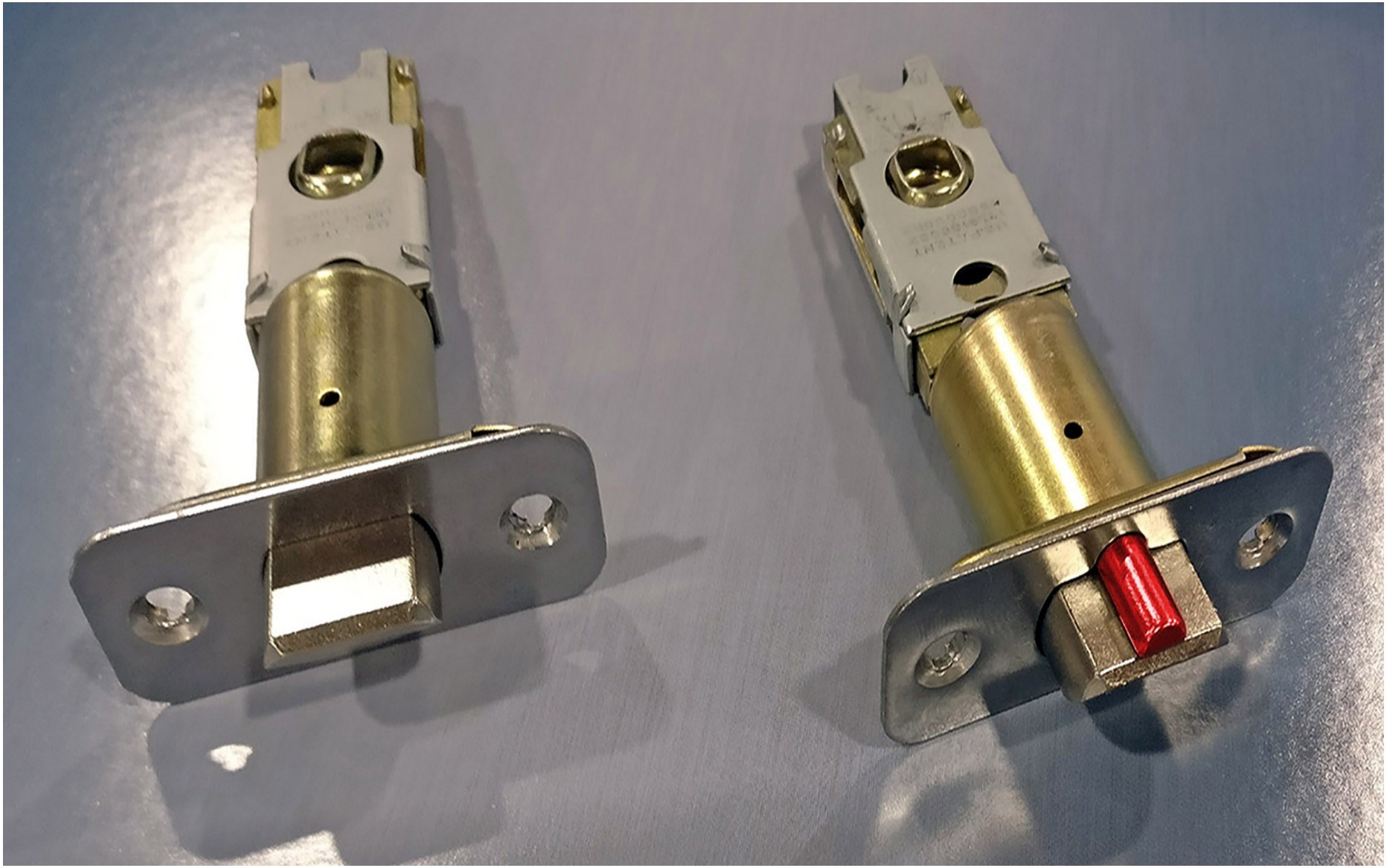


Dead Latches

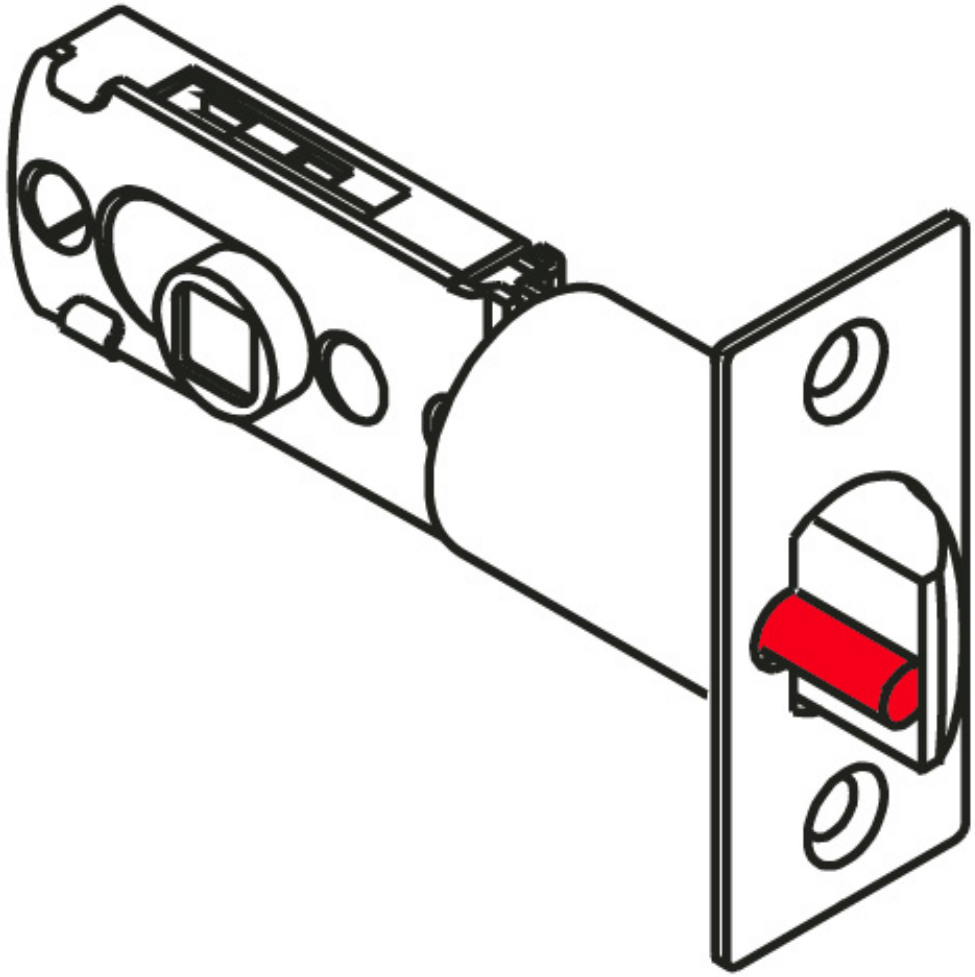
Dead Latches



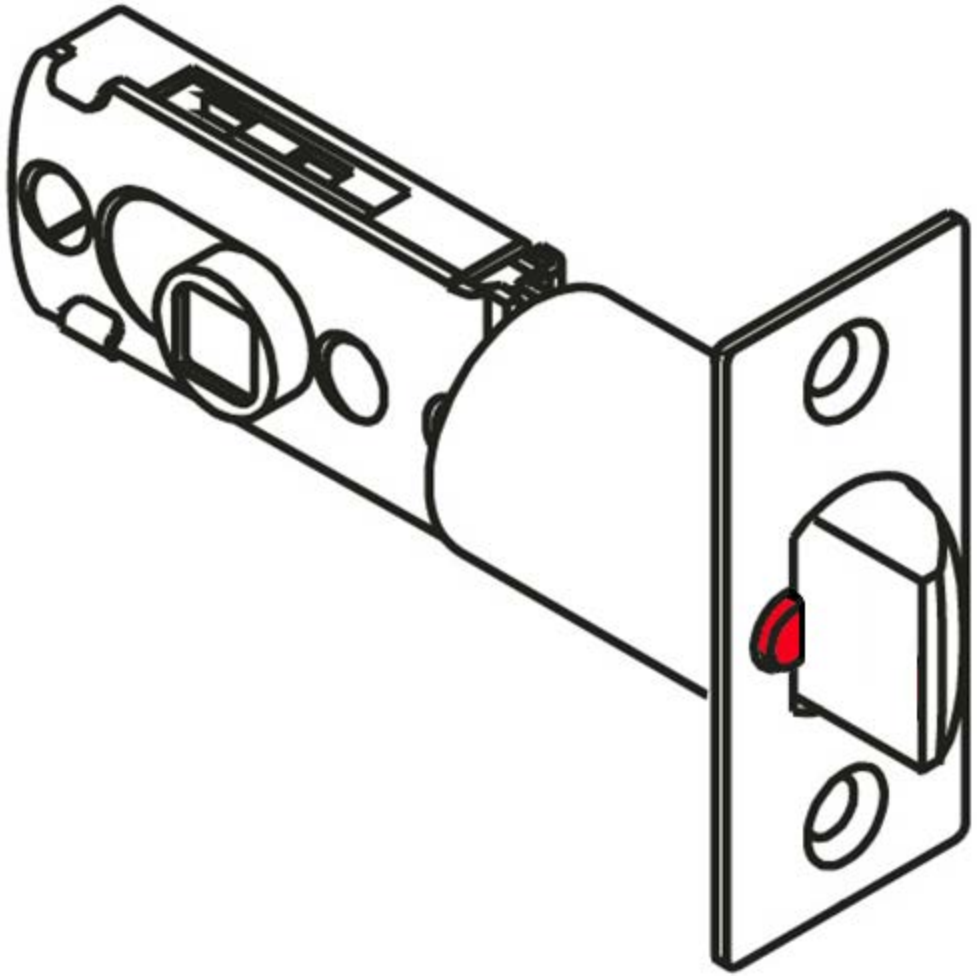
Dead Latches



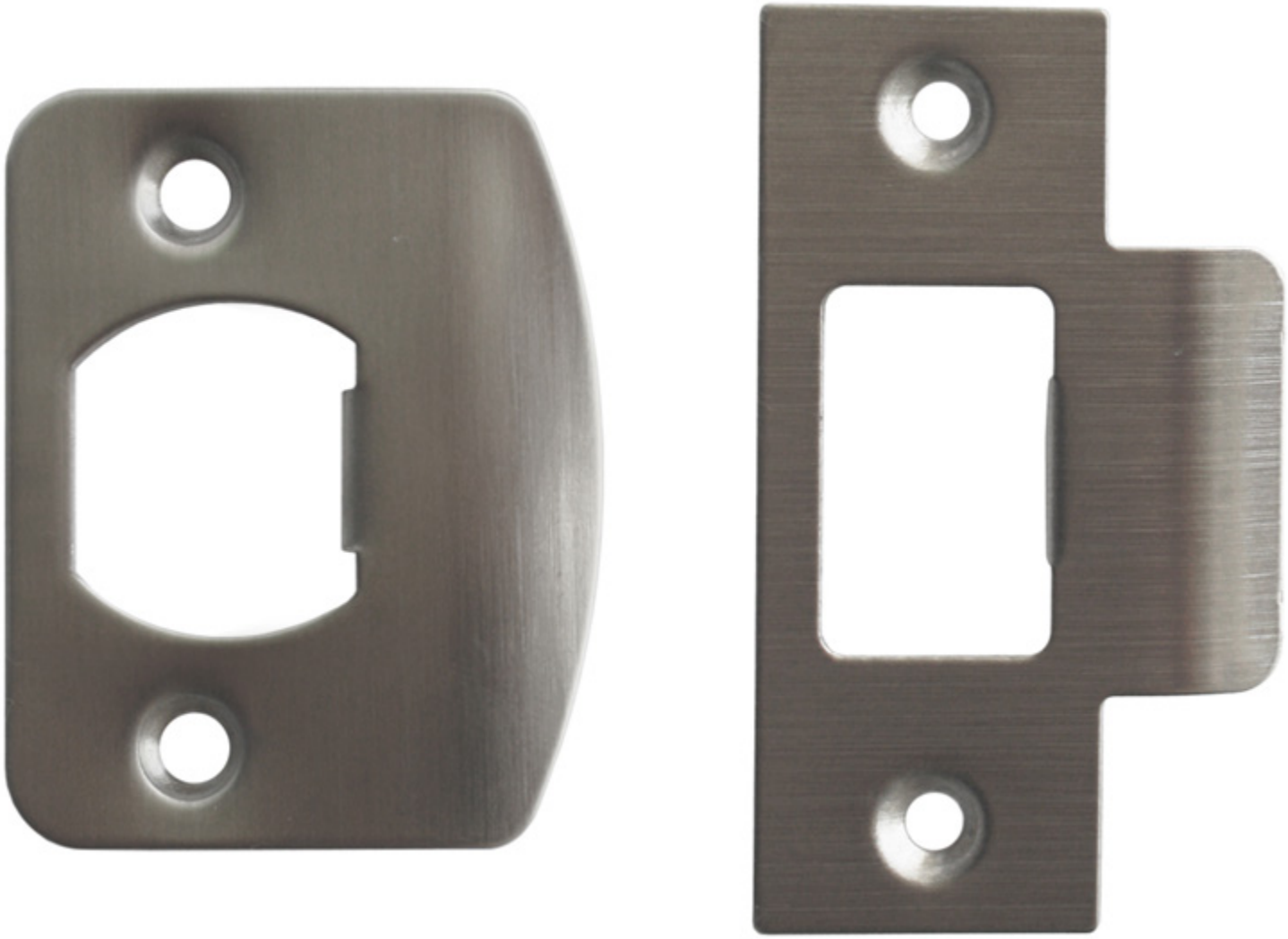
Dead Latches



Dead Latches



Dead Latches Rely on Proper Door Fitment



Door Fitment

Door Fitment

Door Fitment

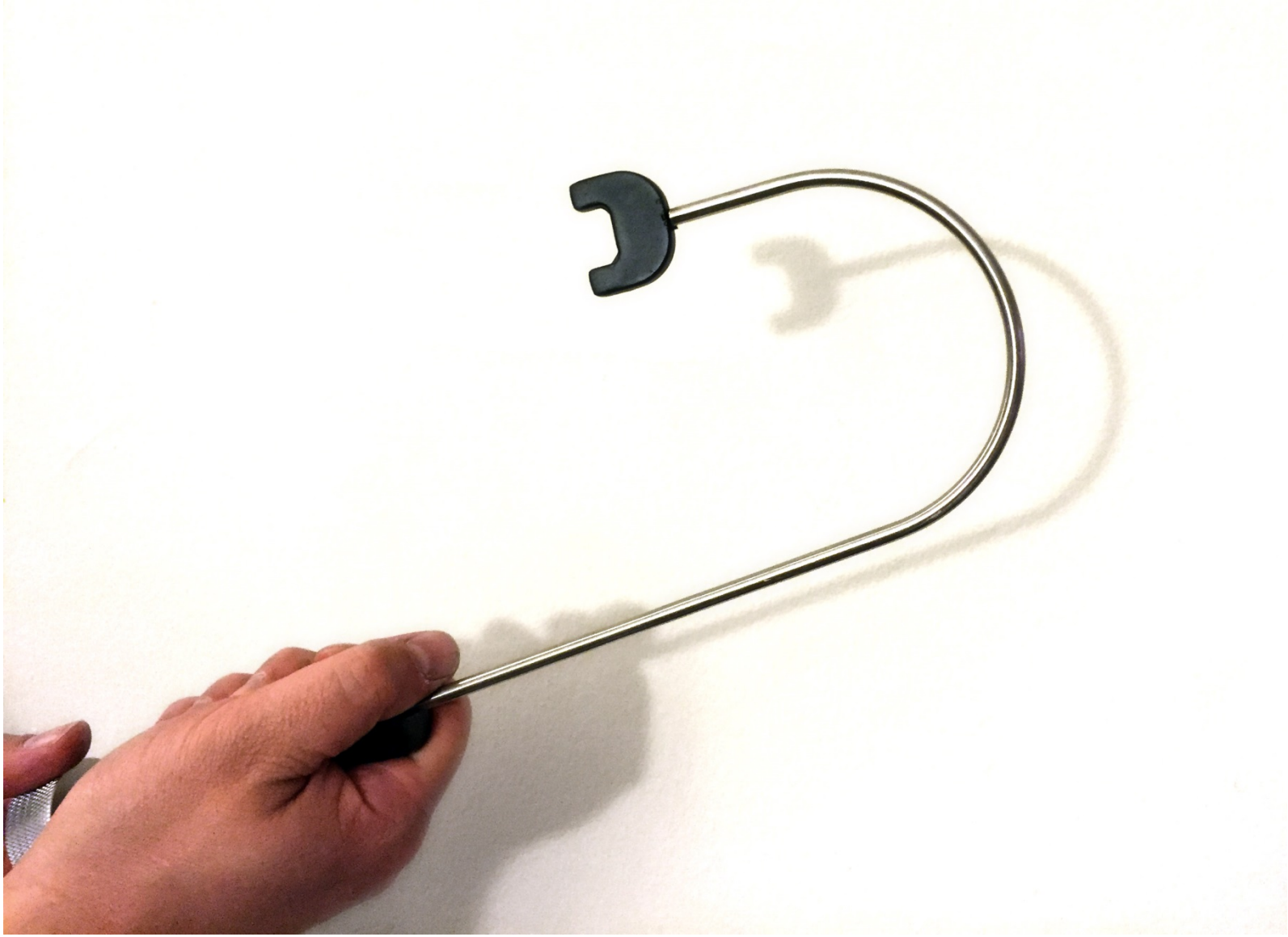
Door Fitment

Door Fitment

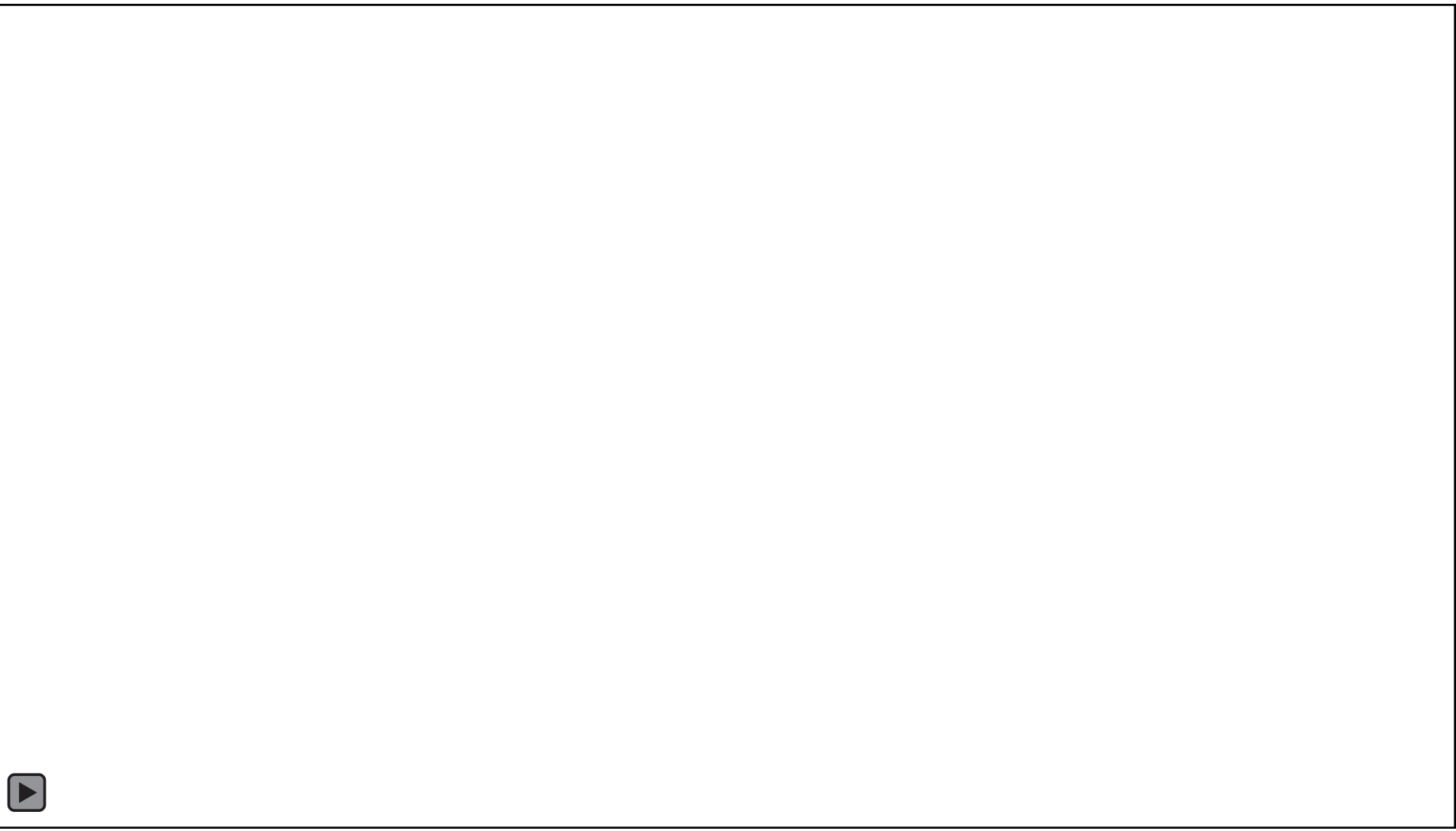
Crash Bars

Deadbolt with Thumb Turn

Thumb Turn Flipper

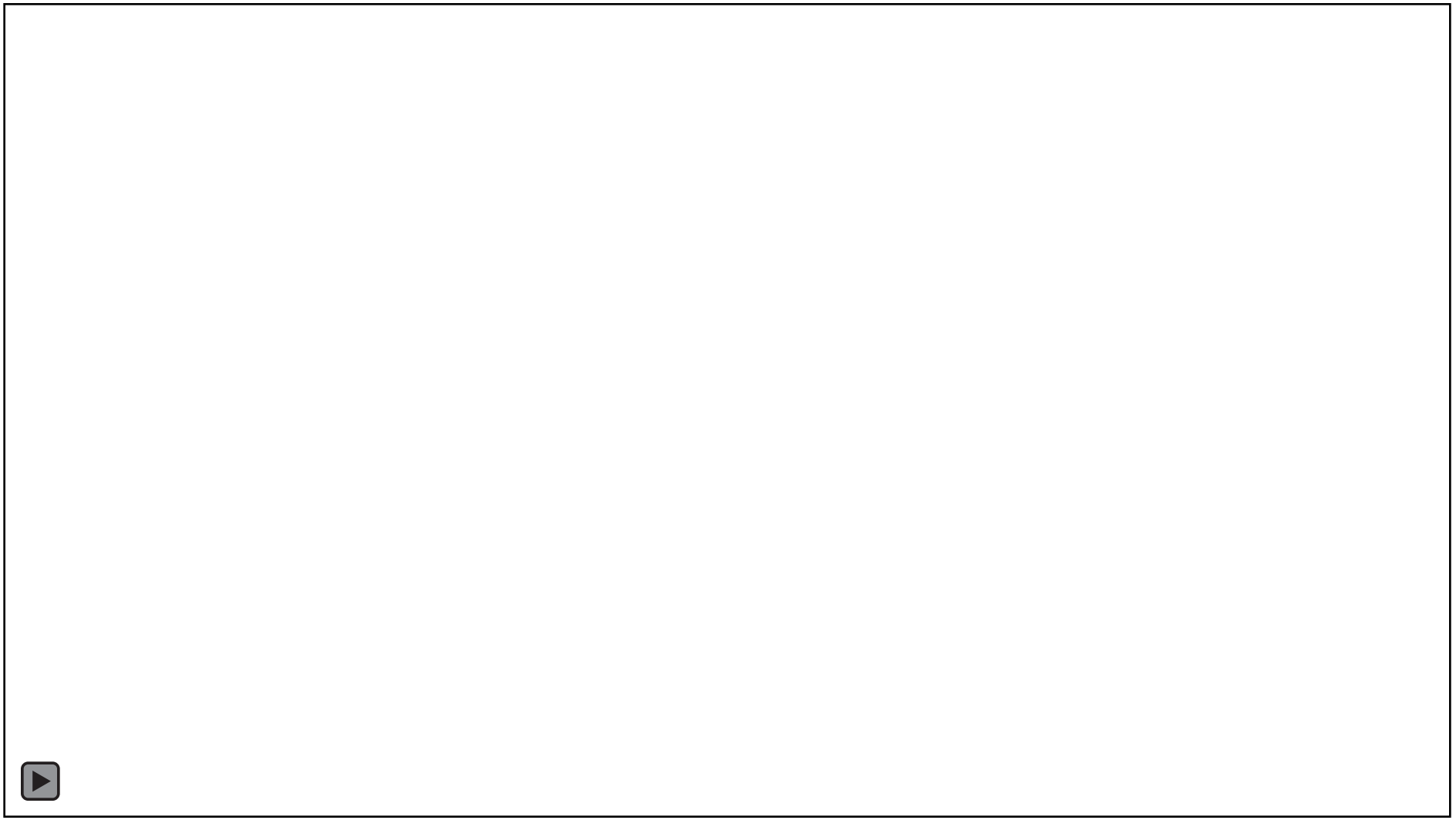


Thumb Turn Flipper



Door Bypassing – Thumb Turn Flipper

Door Bypassing – Thumb Turn Flipper



Edge Gaps and Motion Sensors

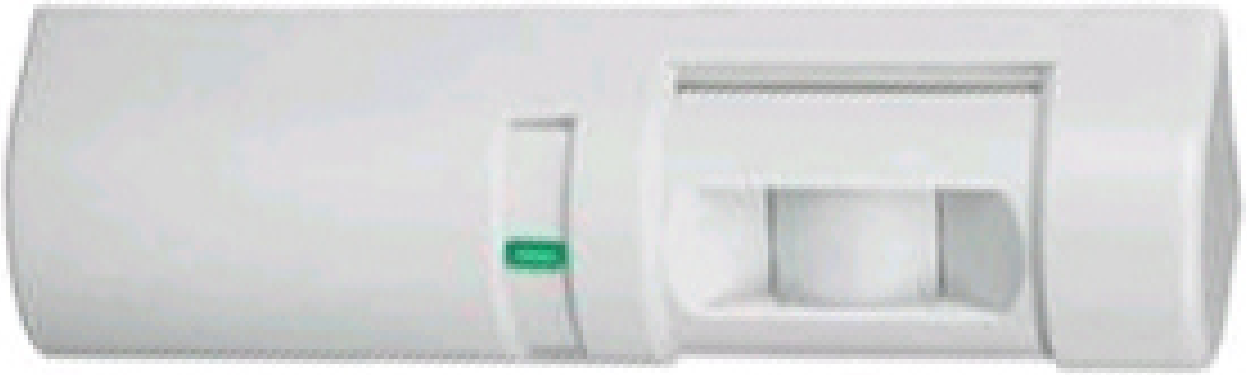
Edge Gaps and Motion Sensors

Edge Gaps and Motion Sensors

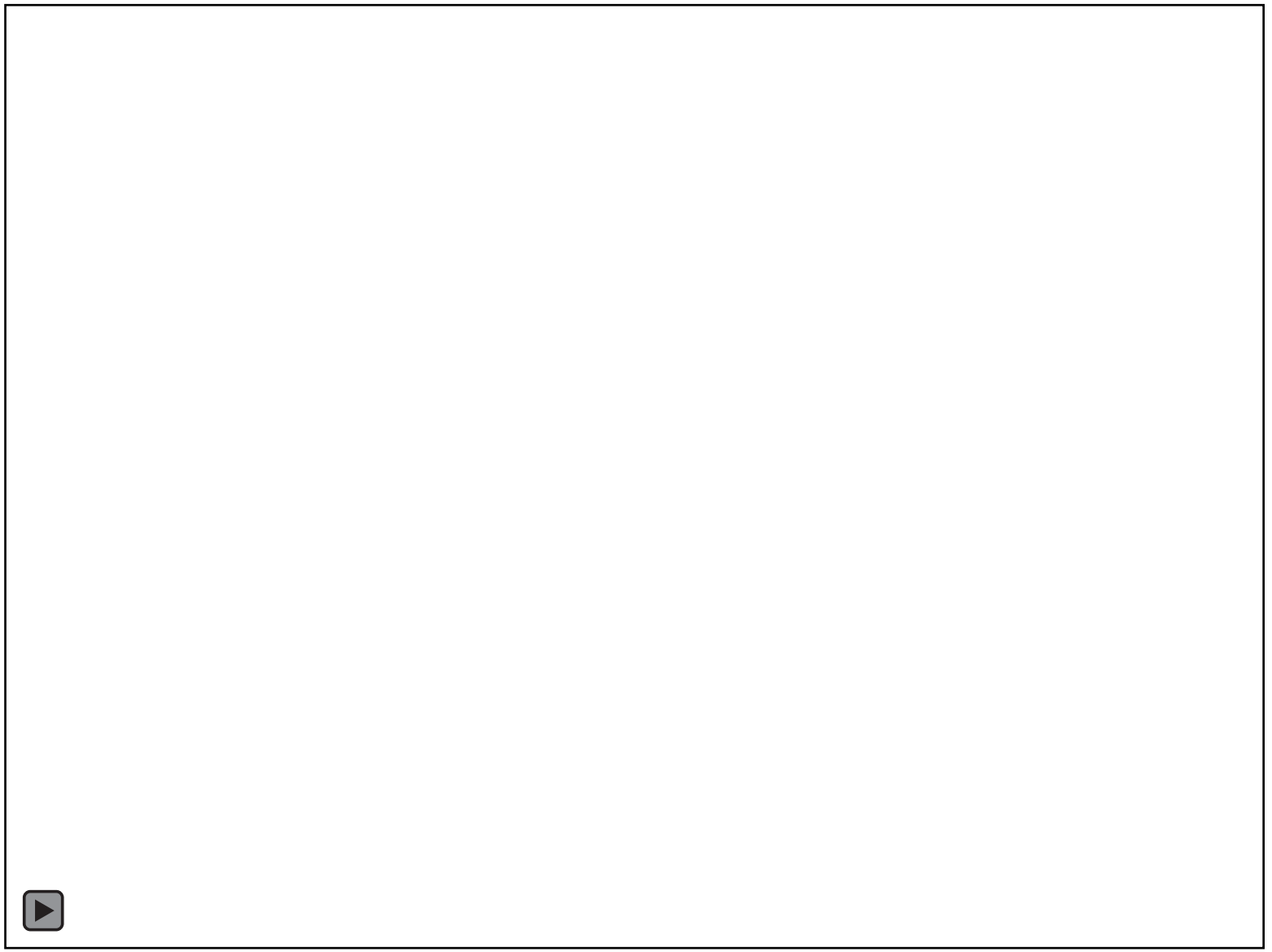
Edge Gaps and Motion Sensors

Edge Gaps and Motion Sensors

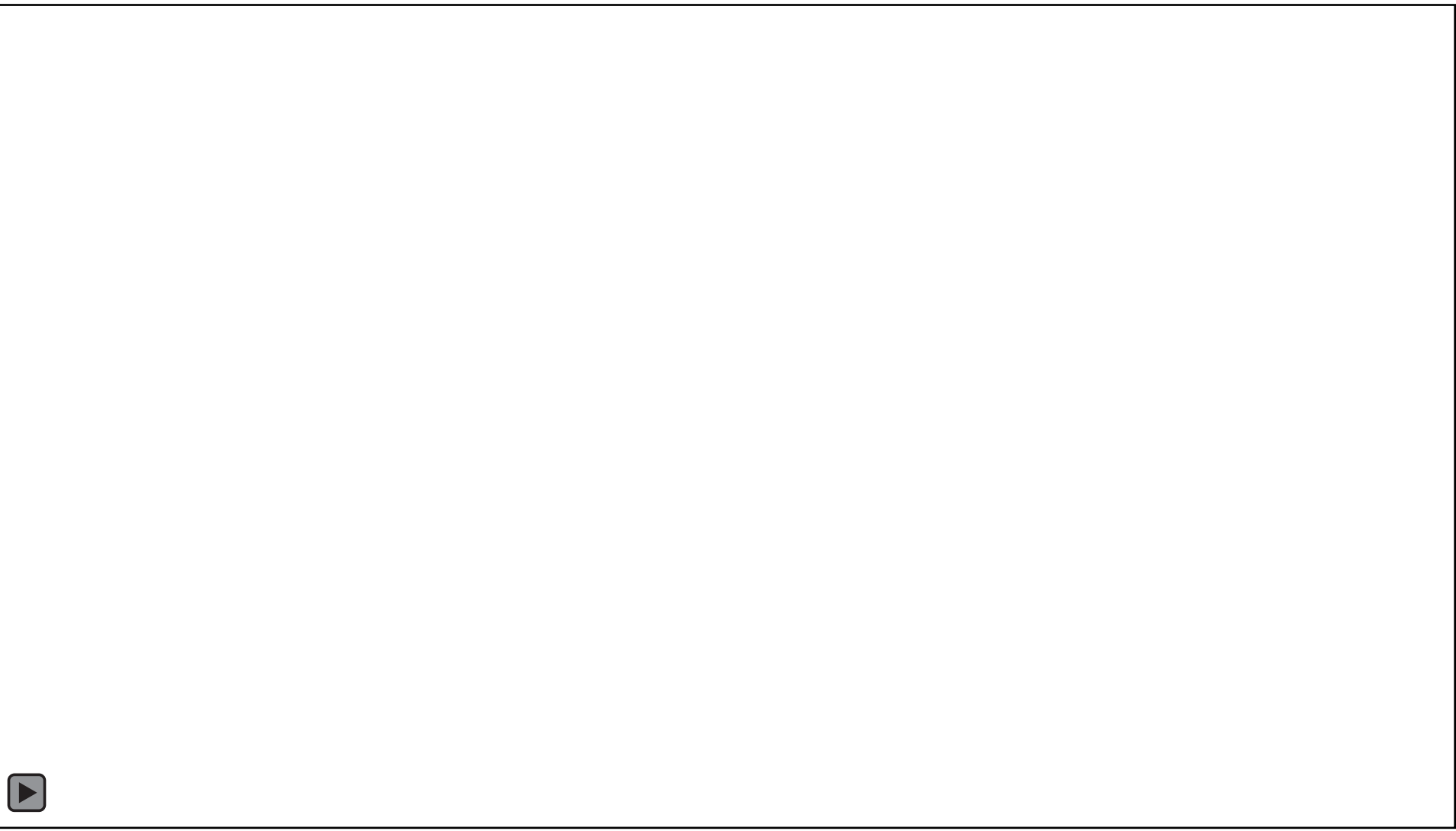
Request-to-Exit (REX) Sensors



Request-to-Exit (REX) Sensors



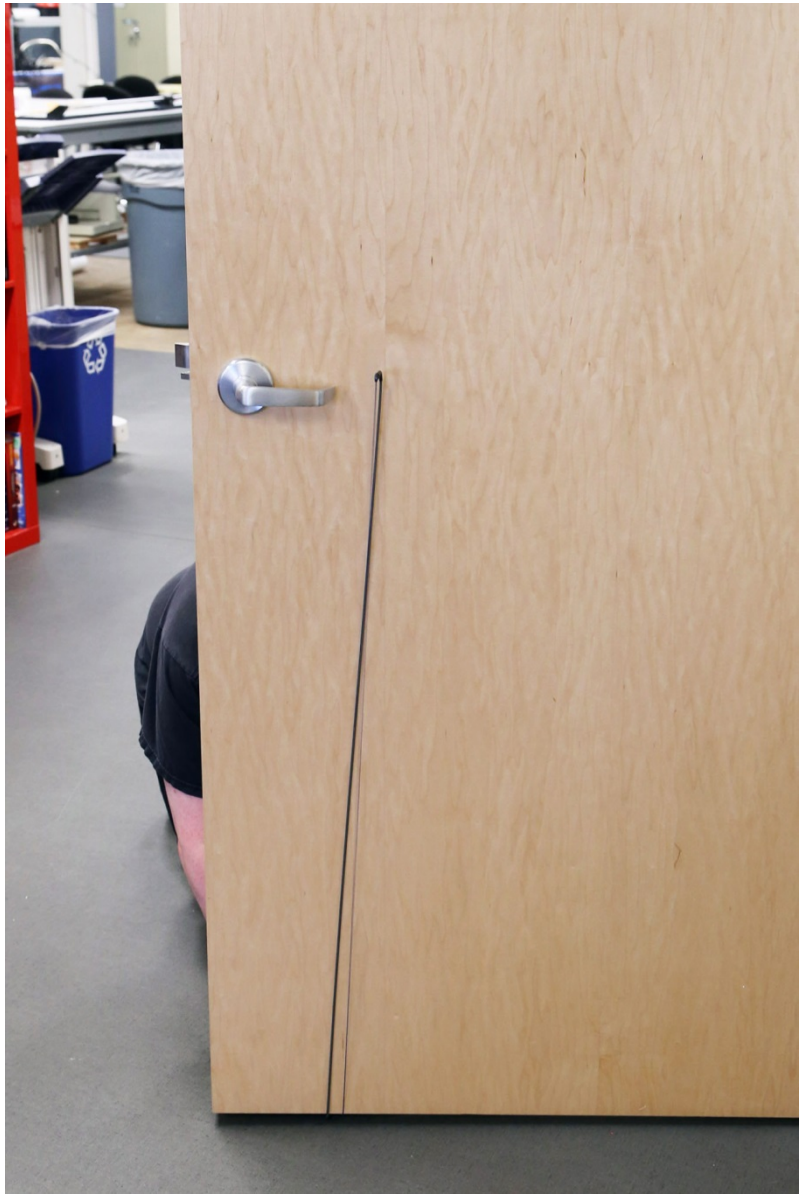
Request-to-Exit (REX) Sensors



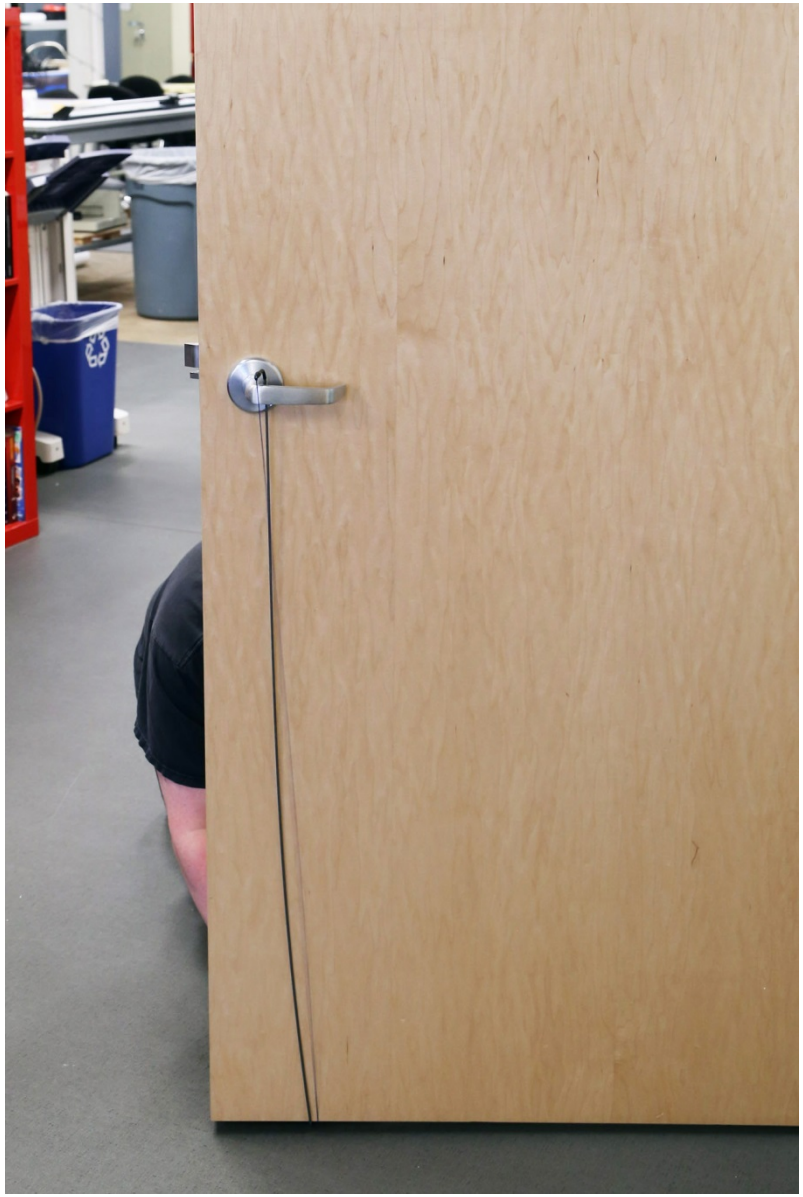
Modern Door Lever Style Handles

Under Door Attacks

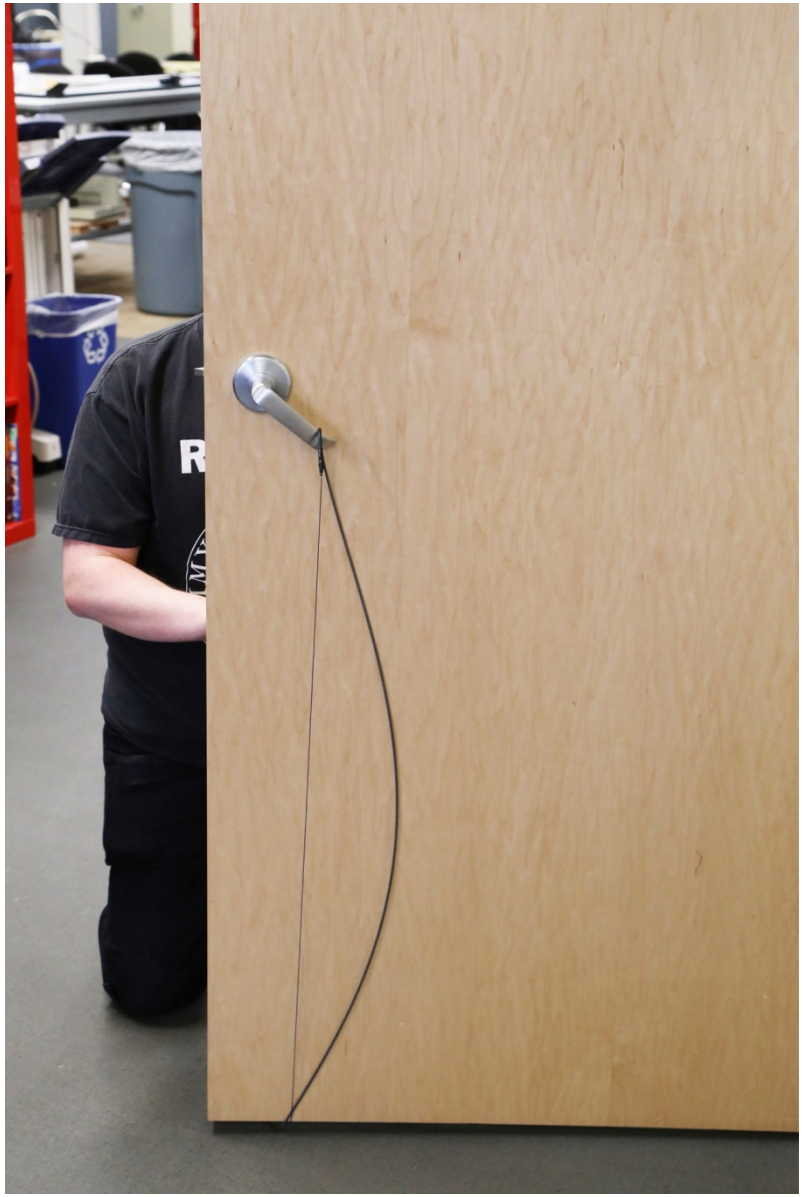
Under Door Attacks



Under Door Attacks



Under Door Attacks



Under Door Attacks

Under Door Attacks

Under Door Attacks

Under Door Attacks

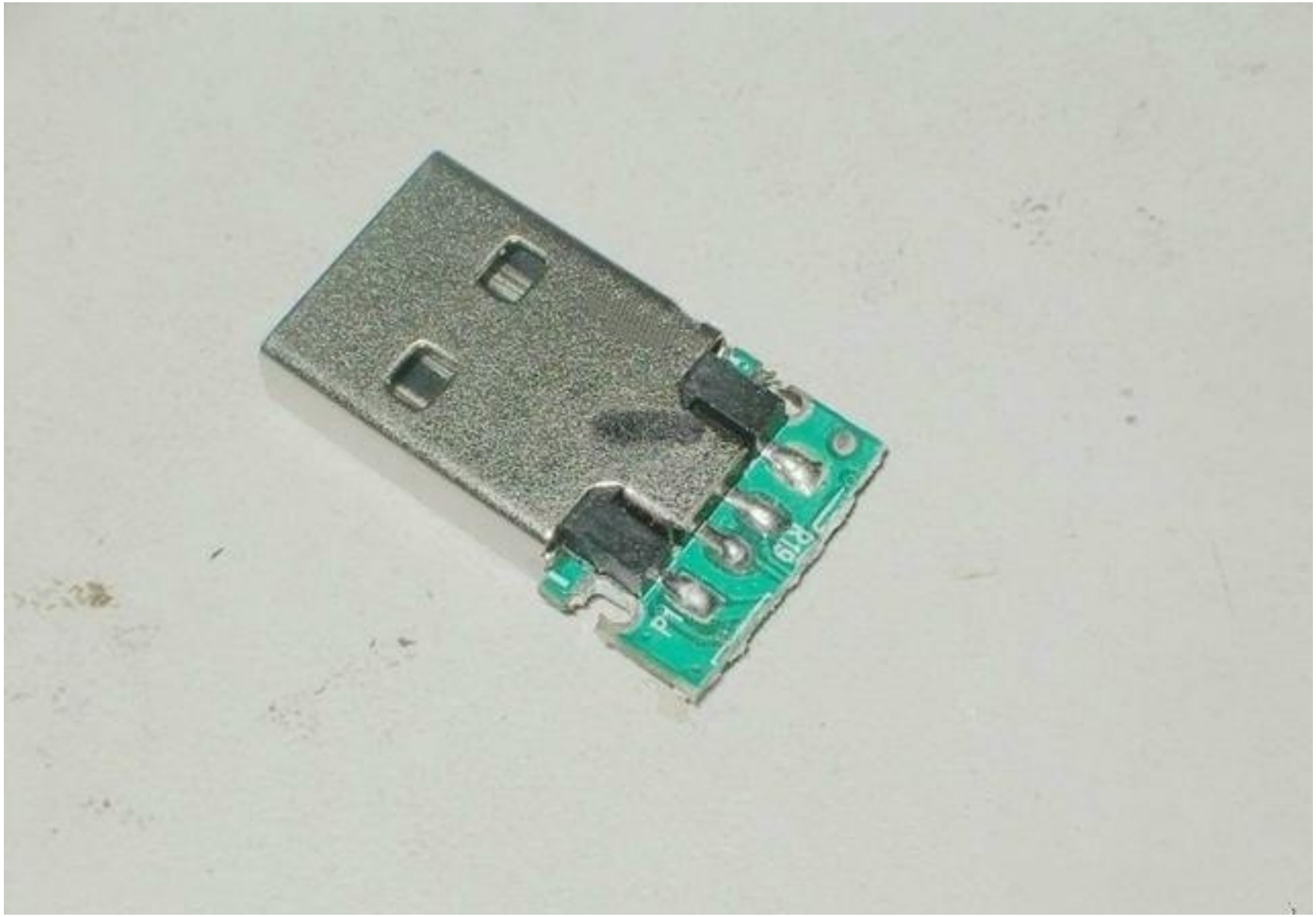
Social Engineering is a Major Factor

Training the Humans

Training the Humans

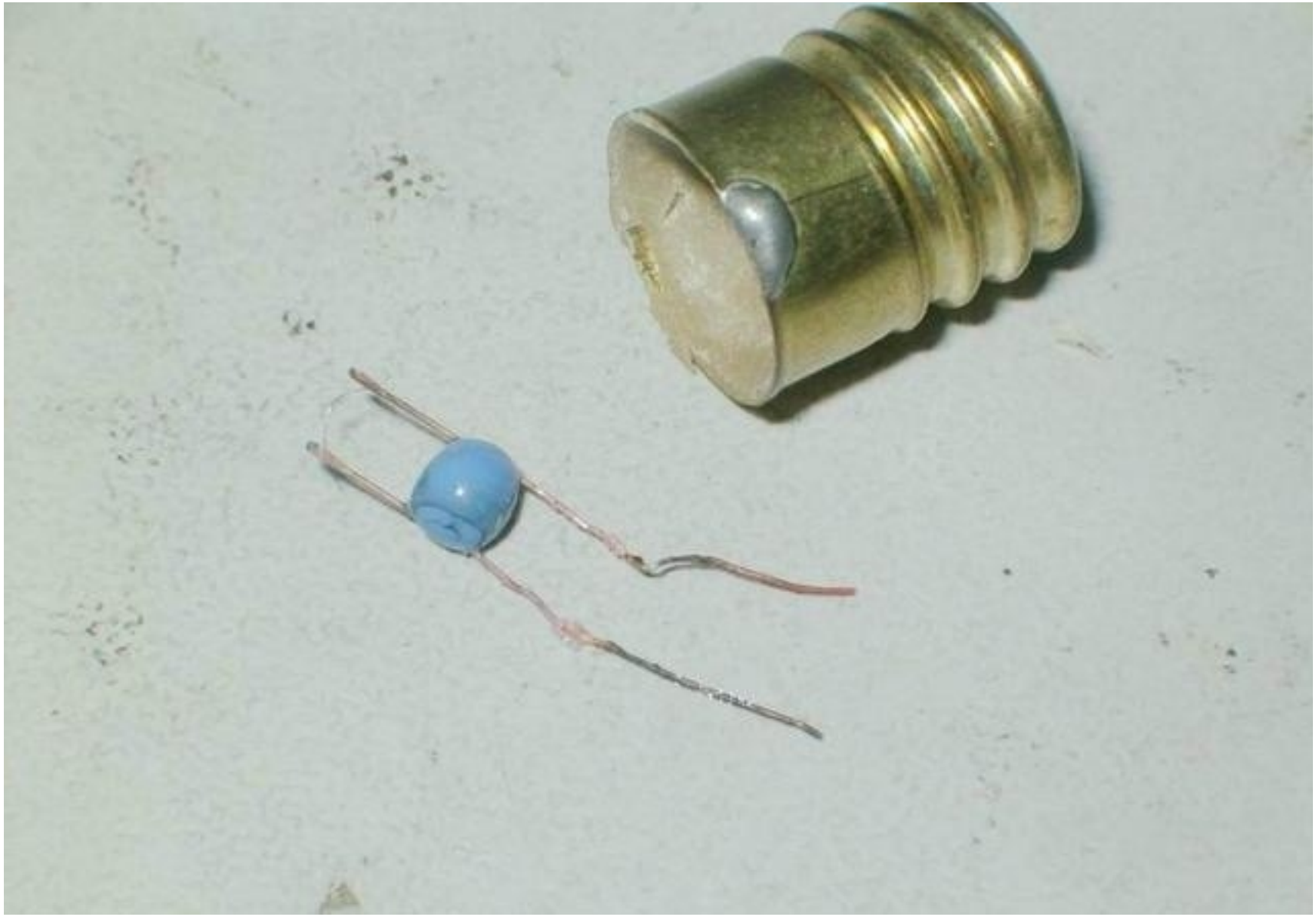
Training the Humans

Training the Humans

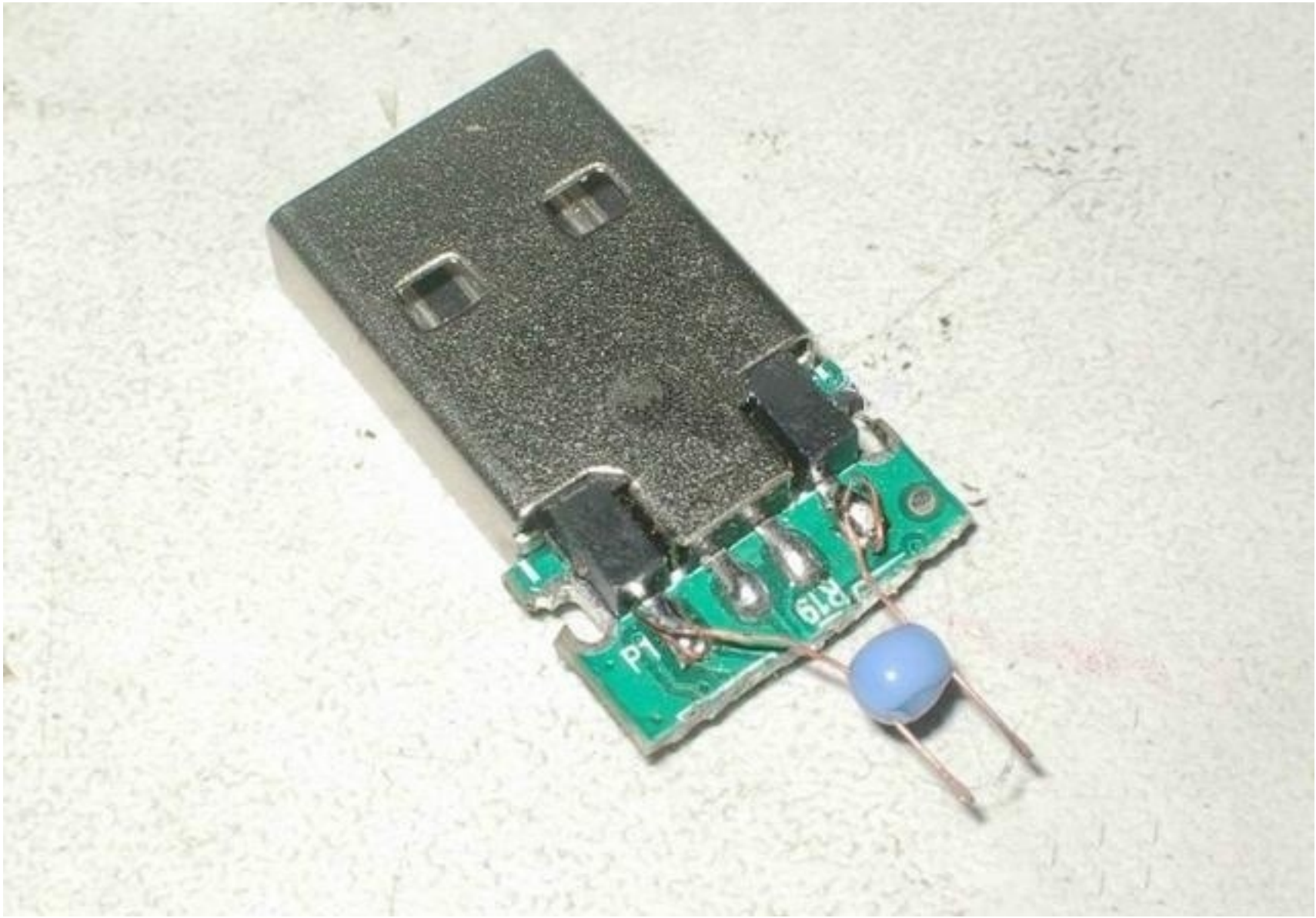


Training the Humans

Training the Humans



Training the Humans



Training the Humans

Training the Humans

Training the Humans

Training the Humans

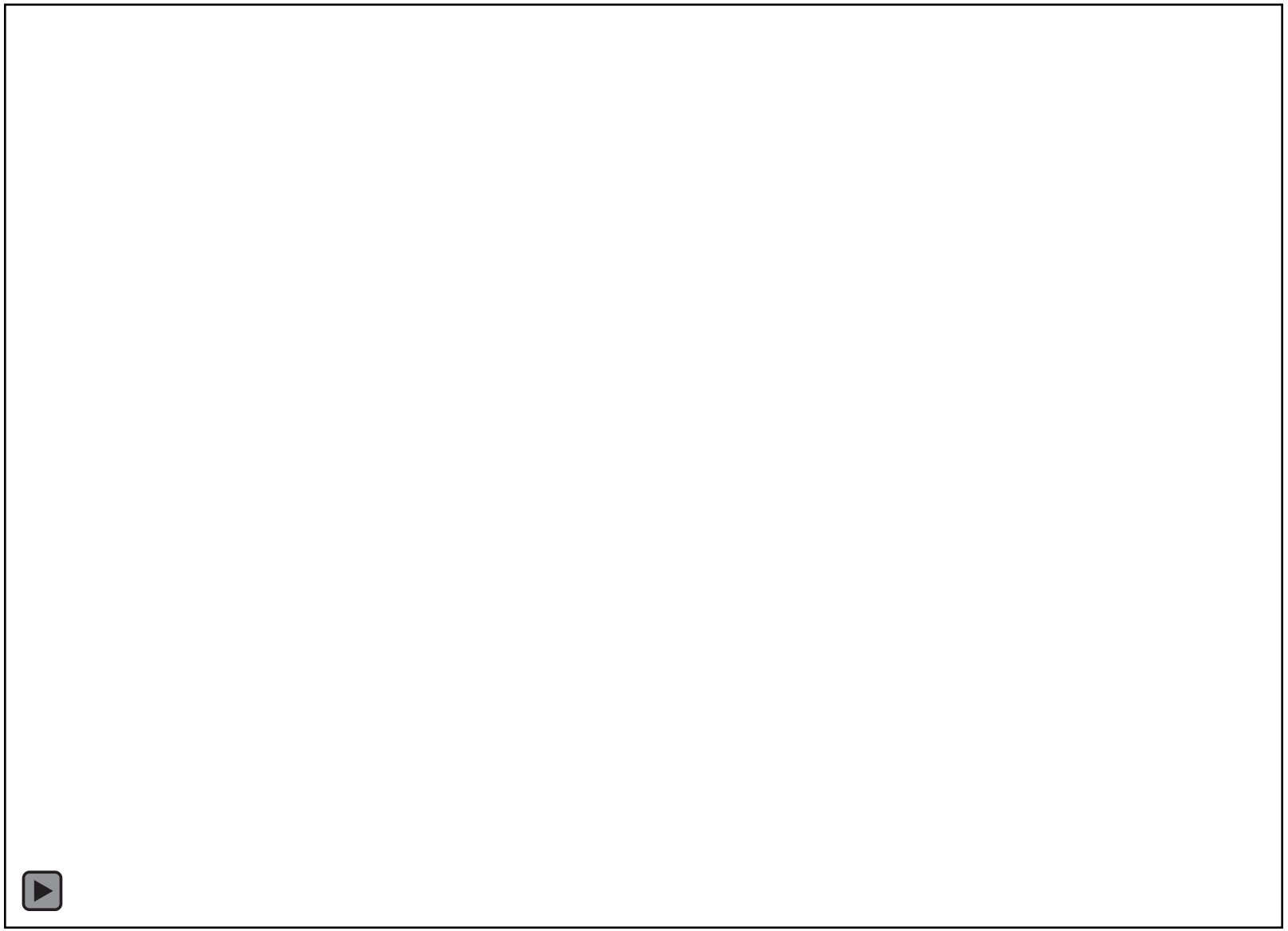
Training the Humans

Training the Humans

Humans as the Attack Vector

Just Look Like You're Busy Working

Just Look Like You're Busy Working



Story Number One – Elevator Repair

We Entered the Building by Attacking a REX Sensor

Elevator Technician is a Great Cover Story

A Metal Contractor Clipboard is Awesome, By The Way

A Metal Contractor Clipboard is Awesome, By The Way

A Metal Contractor Clipboard is Awesome, By The Way

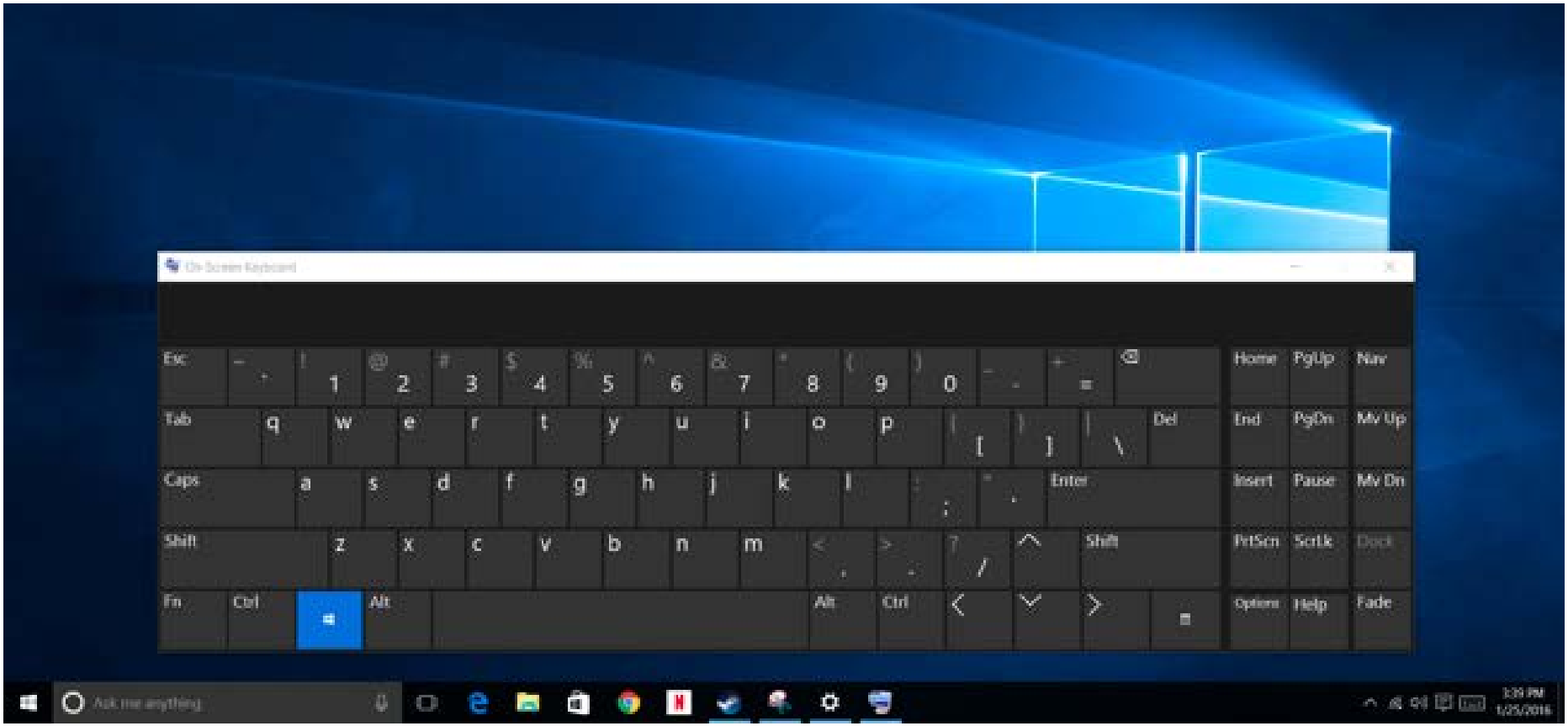
Teammate Had to Go Back to Hotel

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
Please use the North Wing elevator bank
1 - LOWER LEVEL
ST AVE SW
2 - MAIN LOBBY
ND AVE SW
FLOOR 3
FFICE CENTER
OR 4 THRU 6
OFFICES

Fortunately, I'm a Friendly Elevator Technician

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

Who Wouldn't Want to Keep the Elevators Working?

Story Number Two – The Armed Guards

Most of the Time, Guards are Rather Untrained

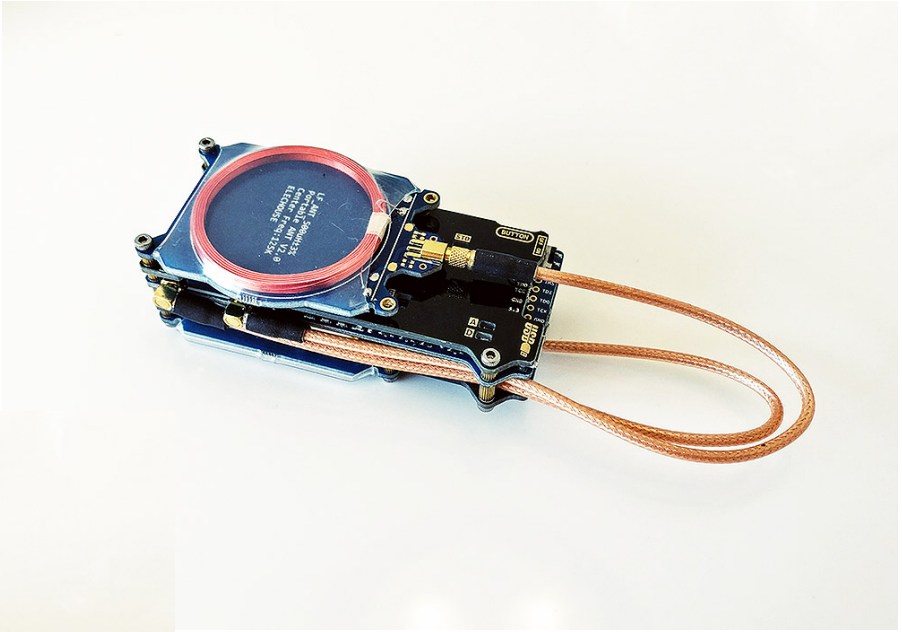
Most of the Time, Guards are Rather Untrained

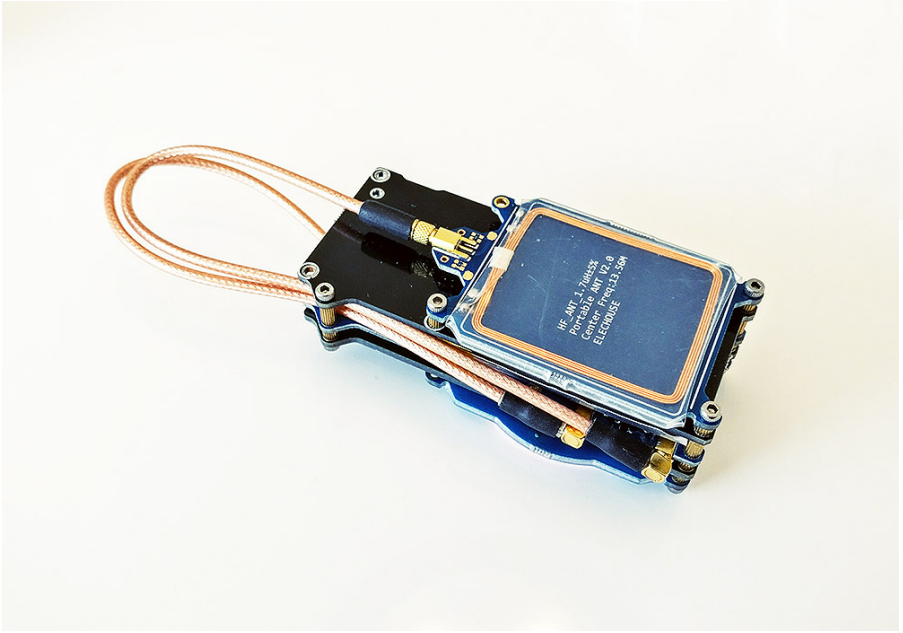
Most of the Time, Guards are Rather Untrained

Armed Guards are Usually More On the Ball

We Needed to Grab Credentials

We Needed to Grab Credentials

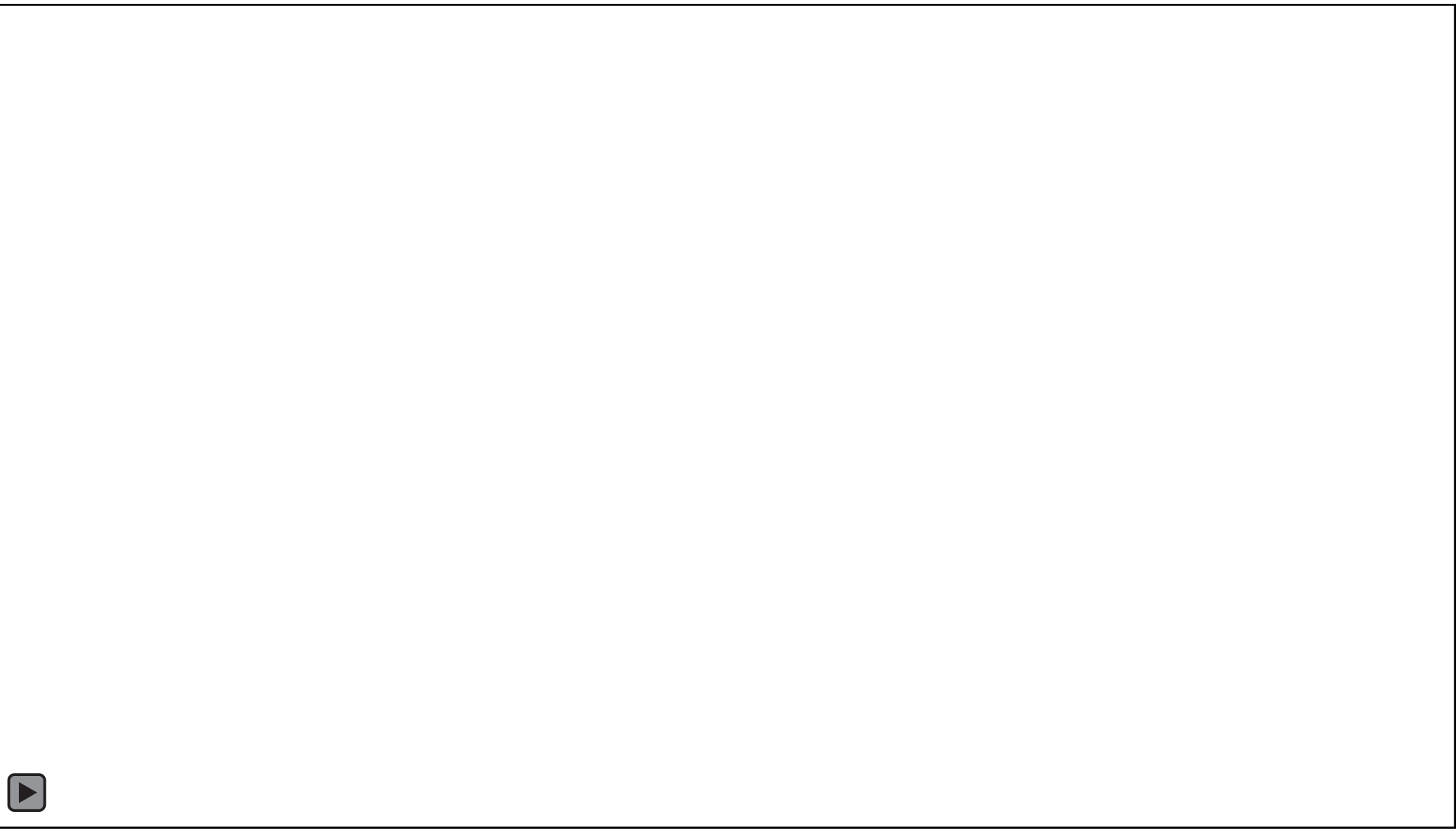




We Needed to Grab Credentials

We Needed to Grab Credentials

We Needed to Grab Credentials

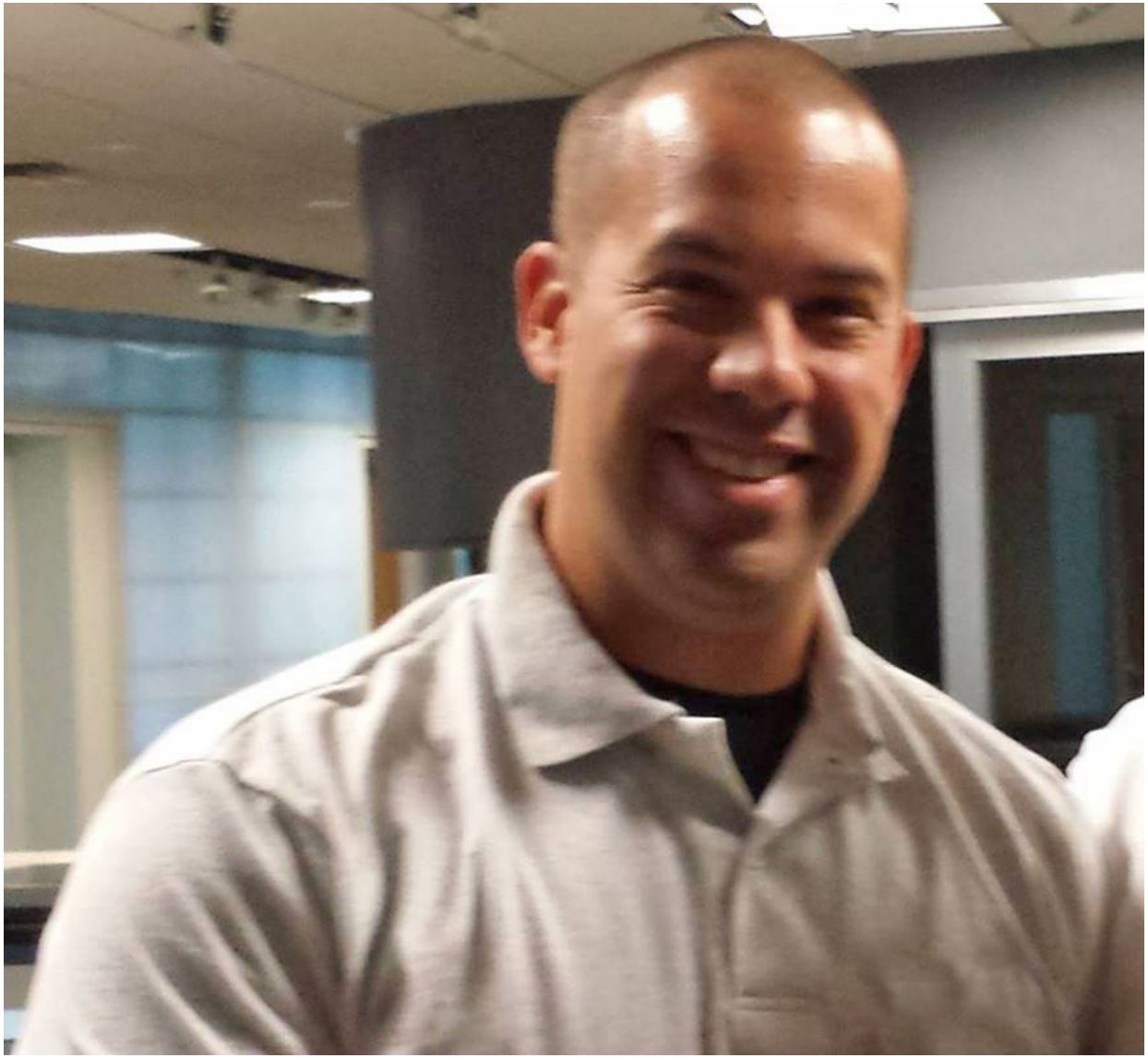


We Needed to Grab Credentials

What Does Every Armed Guard Think About Becoming?

What Does Every Armed Guard Think About Becoming?

Send in a Cop!



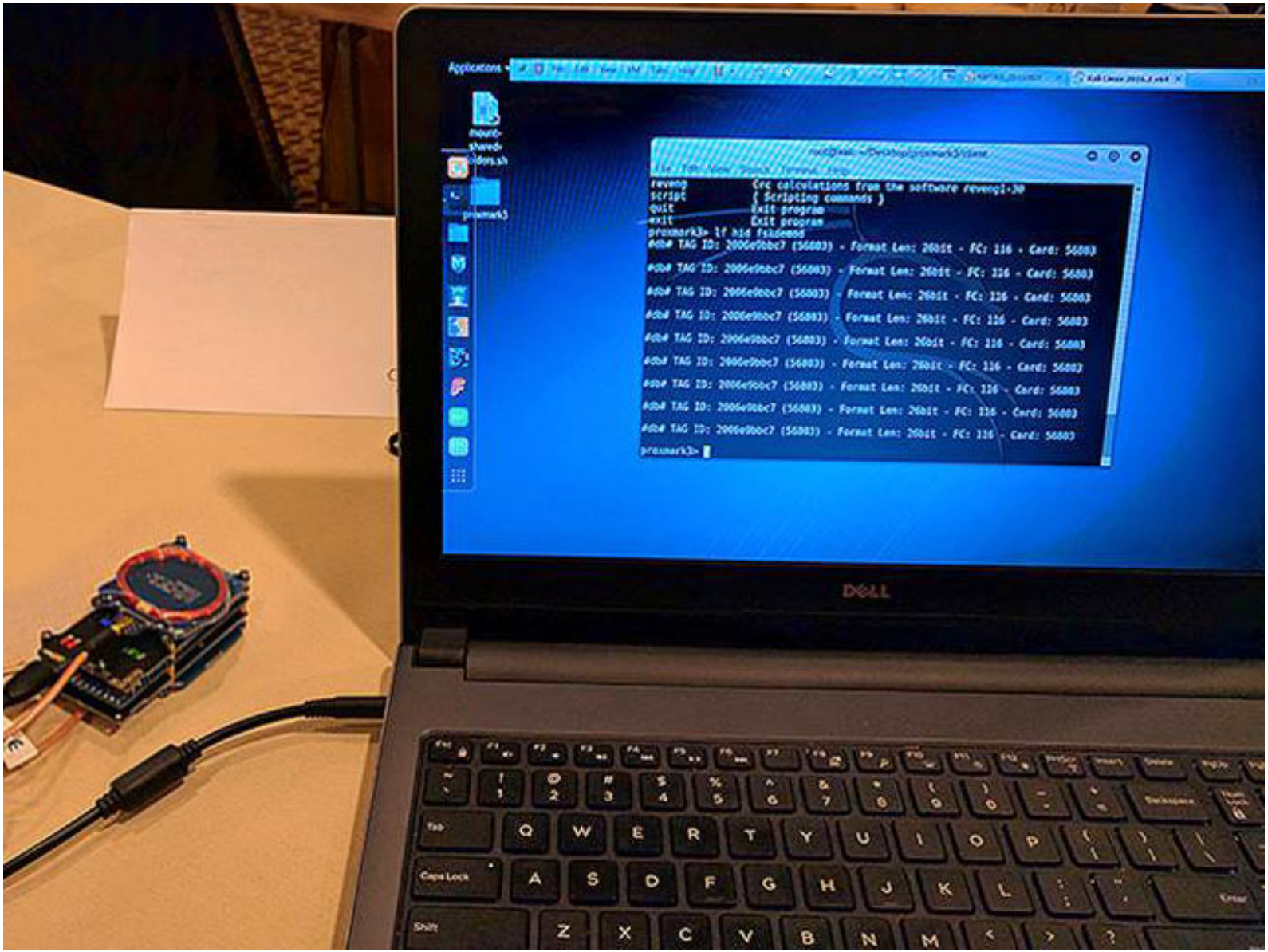
Meanwhile, Babak is Still Out in the Car

Rob Keeps Trying, The Guards Keep Blading

Time to Wrap it Up and Say Goodbye

Surprise Hug!

We Checked the Logs



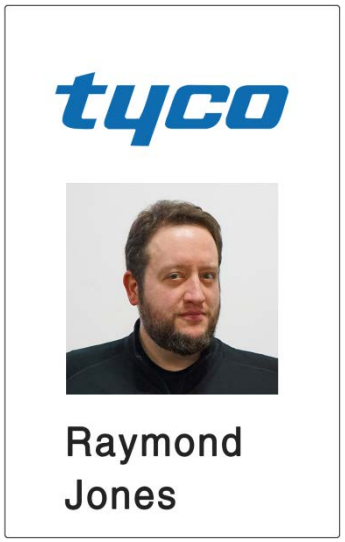
Now Whose Permissions Did We Have?

Story Number Three – The Cable Technicians

Social Engineering Recon

Social Engineering Artistry

Social Engineering Artistry



The Cable Technicians

The Cable Technicians

The Cable Technicians

The Cable Technicians

What Would You Do?

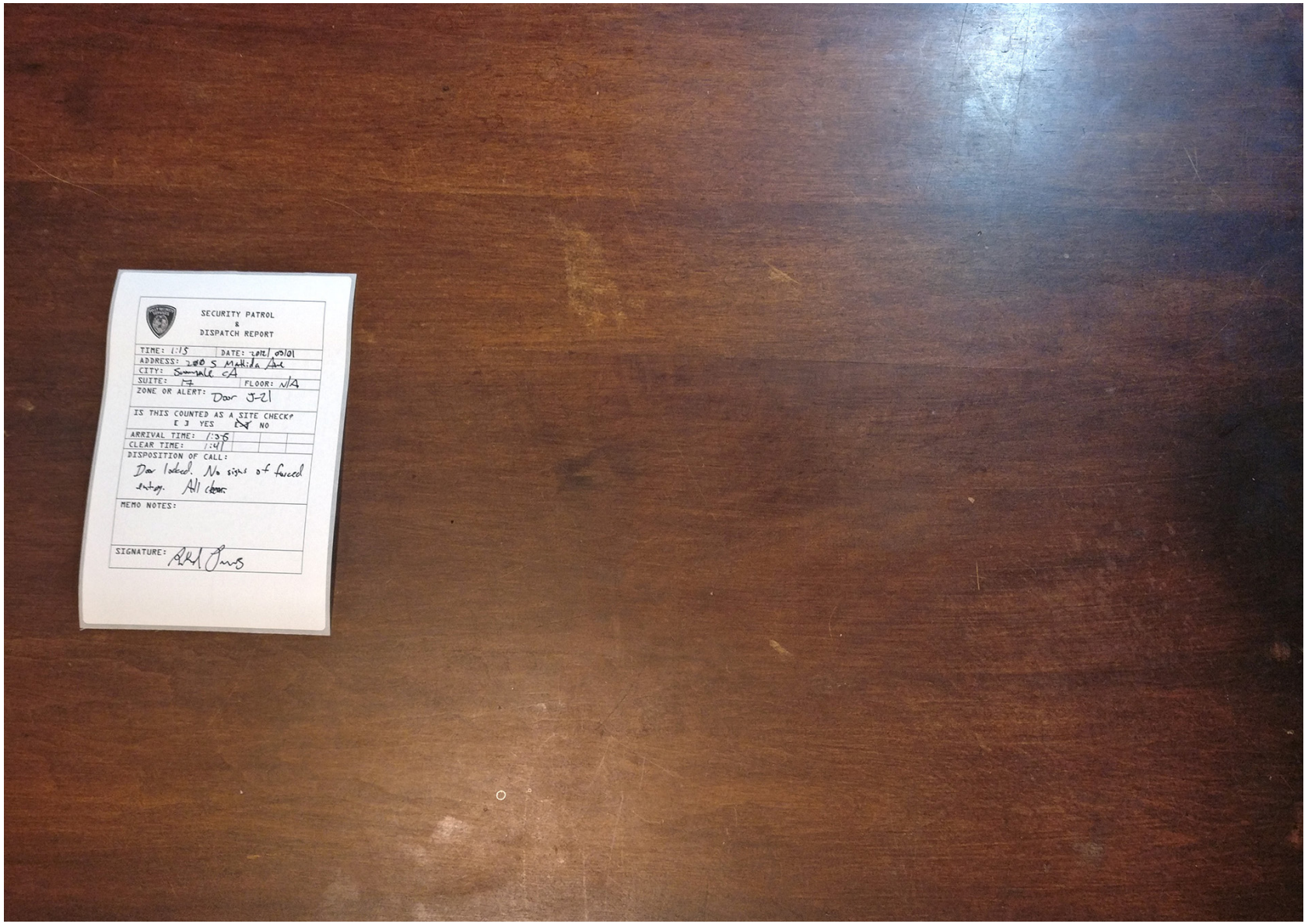
Make a New Friend!

We're Totally Legit... Trust Us.

Do You Think He Verified Our Story?

Later, Inside the Office

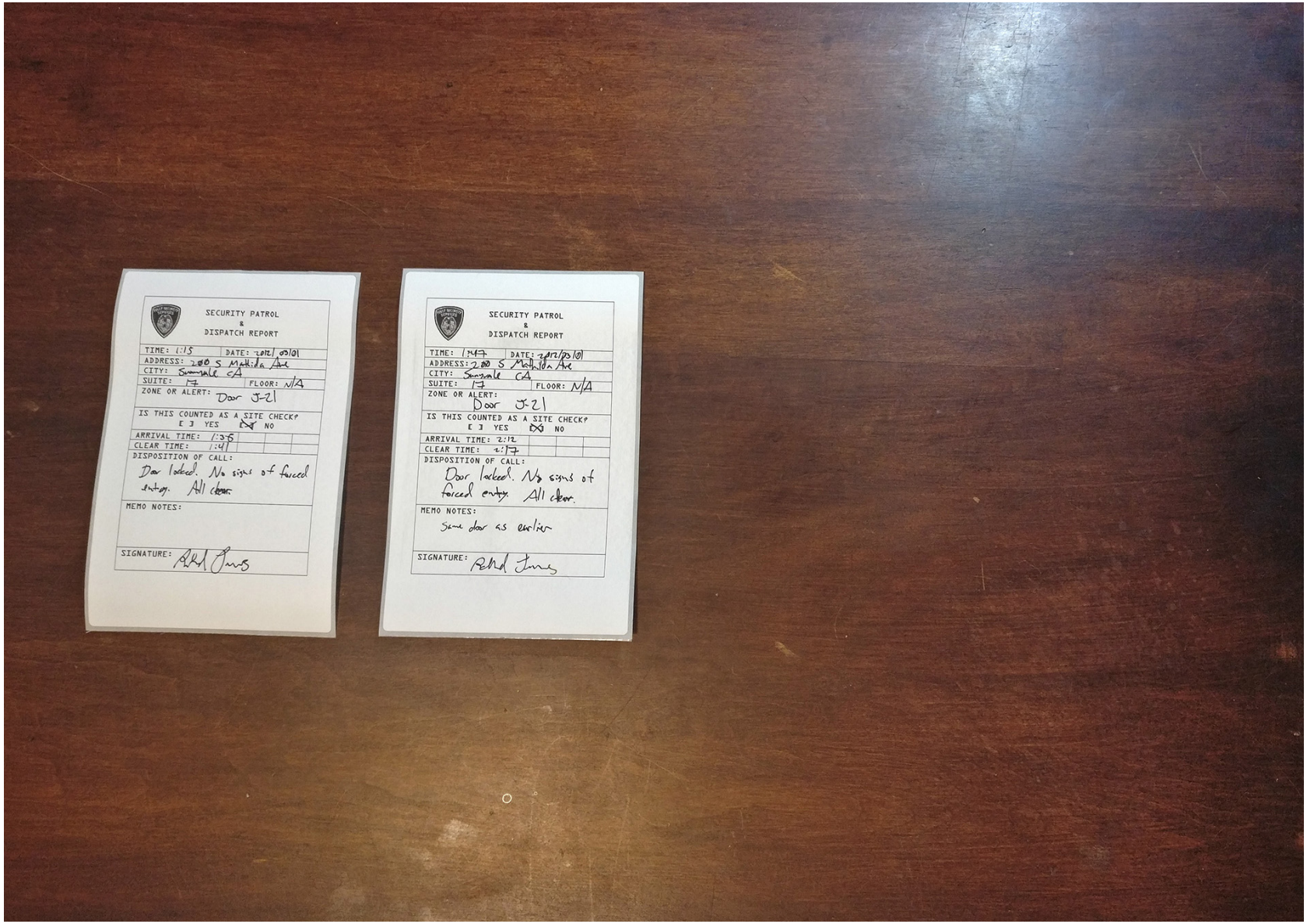
The Client Actually Pulled the Dispatch Tickets



SECURITY PATROL
&
DISPATCH REPORT

TIME: 1:15	DATE: 2012/ 05/01
ADDRESS: 200 S Market Ave	
CITY: Sunnvale CA	
SUITE: 12	FLOOR: N/A
ZONE OR ALERT: Door J-21	
IS THIS COUNTED AS A SITE CHECK? [ ] YES [X] NO	
ARRIVAL TIME: 1:35	
CLEAR TIME: 1:41	
DISPOSITION OF CALL: Door locked. No signs of forced entry. All clear.	
MEMO NOTES:	
SIGNATURE: [signature]	

The Client Actually Pulled the Dispatch Tickets



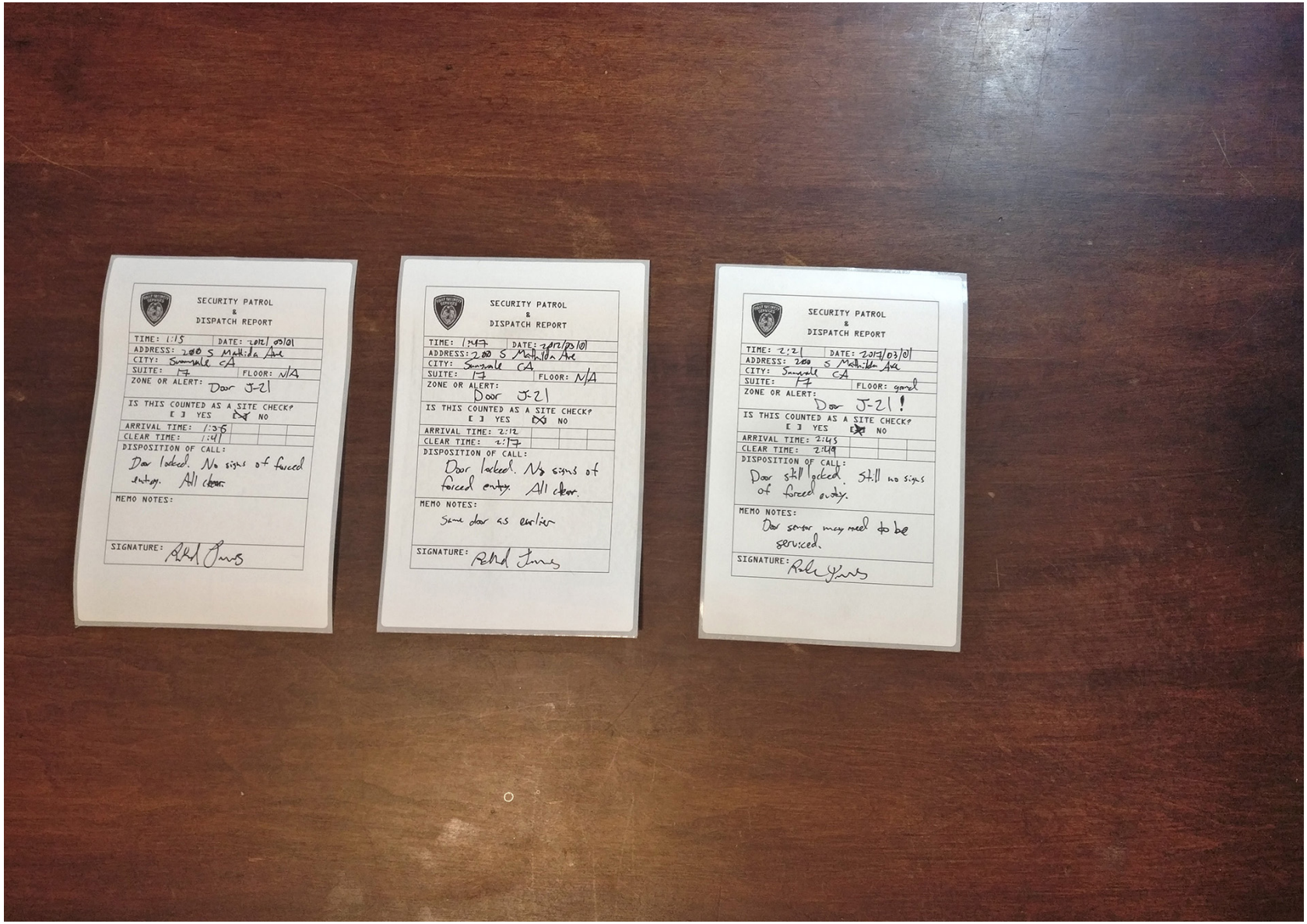
SECURITY PATROL
&
DISPATCH REPORT

TIME: 1:15 DATE: 2012/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 17 FLOOR: N/A
ZONE OR ALERT: Door J-21
IS THIS COUNTED AS A SITE CHECK?
[ ] YES [X] 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 James

SECURITY PATROL
&
DISPATCH REPORT

TIME: 1:47 DATE: 2012/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 17 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: Richard James

The Client Actually Pulled the Dispatch Tickets



The Client Actually Pulled the Dispatch Tickets

SECURITY PATROL & DISPATCH REPORT

TIME: 1:15 DATE: 2012/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 17 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: 2012/03/01
ADDRESS: 200 S Mathilda Ave
CITY: Sunnyvale CA
SUITE: 17 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

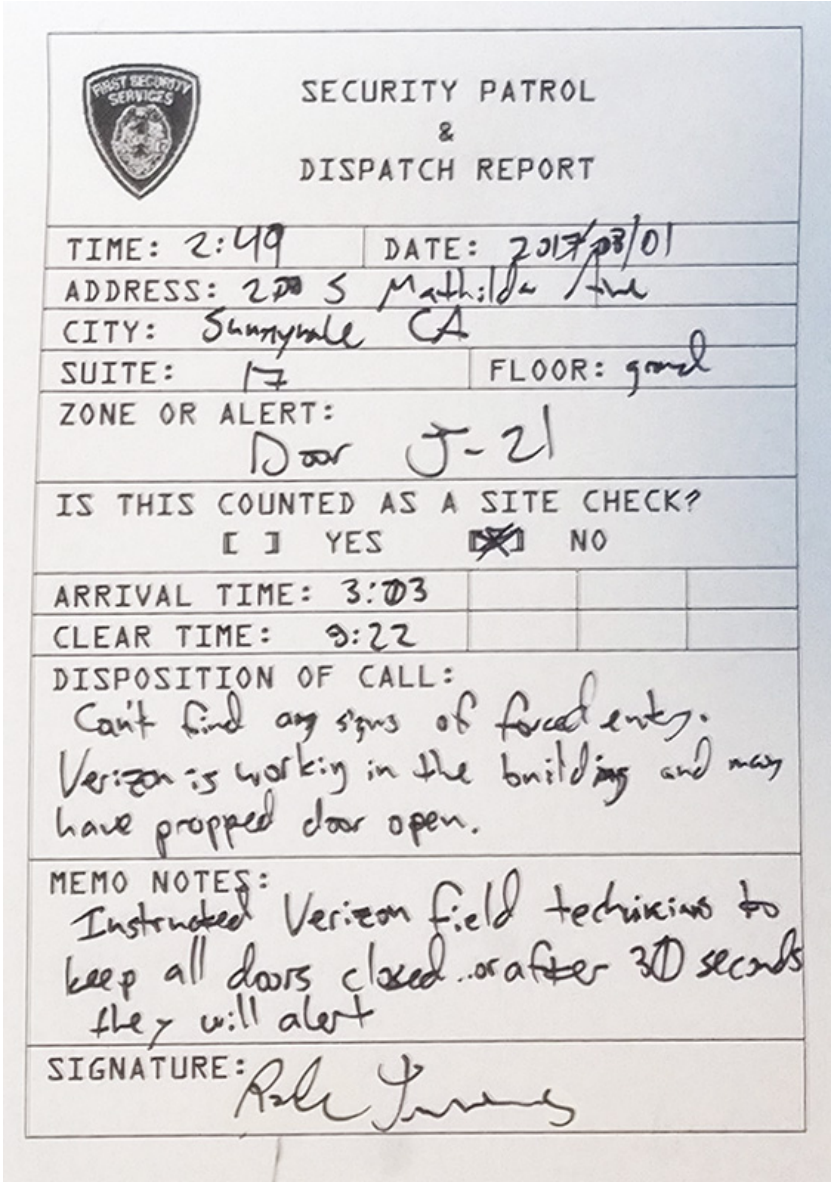
SECURITY PATROL & DISPATCH REPORT

TIME: 2:21 DATE: 2012/03/01
ADDRESS: 200 S 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: 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: 2012/03/01
ADDRESS: 200 S 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 - after 30 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 [illegible]

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]

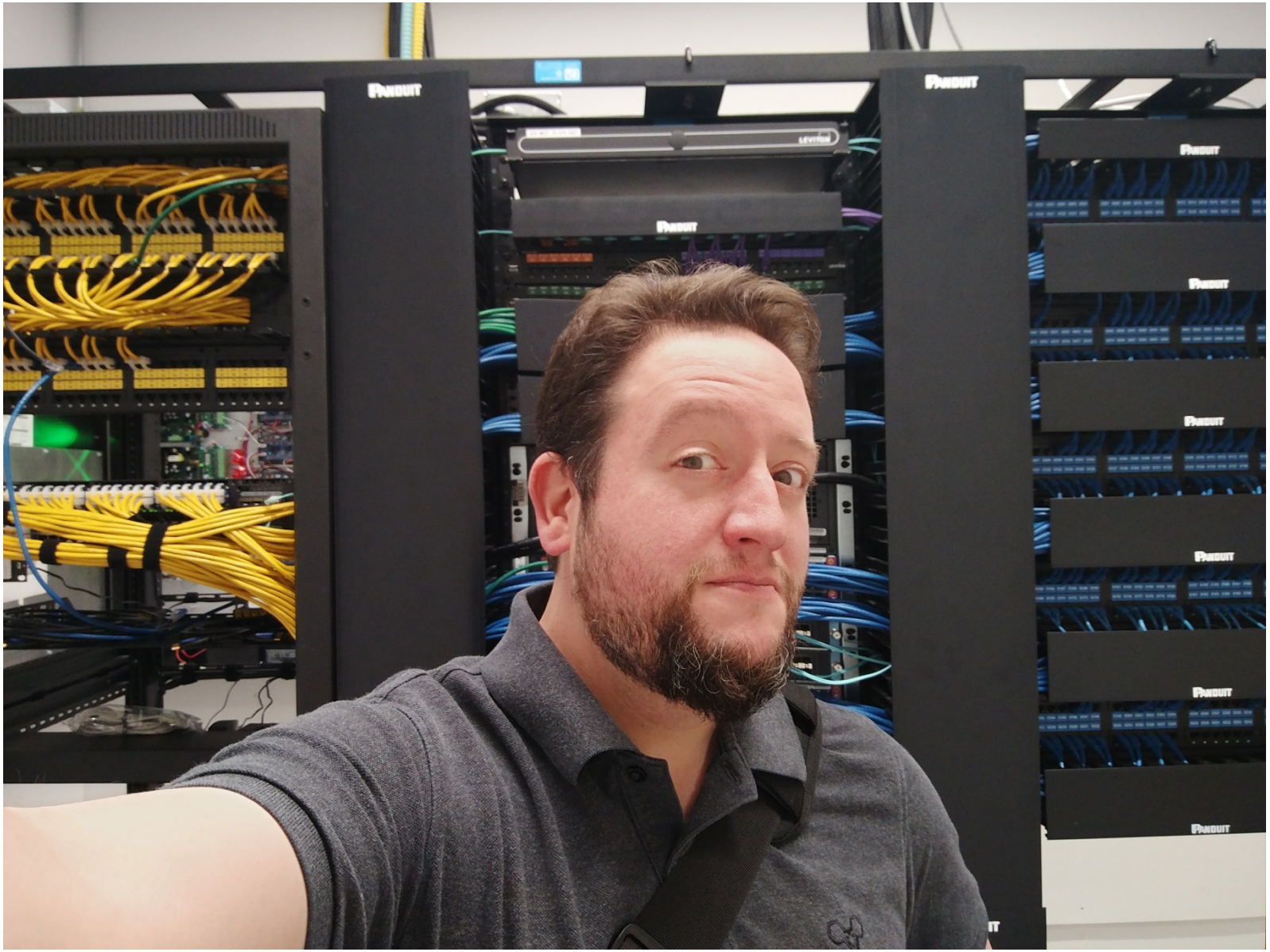
Who Wouldn't Trust Us?

Keep Physical Attacks in Mind

Physical Security is Data Security

Physical Security is Data Security

Physical Security is Data Security



Stay Safe Out There!

Thank You Very Much

delta@enterthecore.net

at the office

@deviantollam

on twitter

“Lagavulin neat”

at the bar