



Can You Murder My City?

(Let's Find Out)

Patrick Lavery
@plaverty9
Plaverty@CompassCyberGuard.com

A Quick Note

- This is a 2-hour story
- Details omitted
- Fun stuff included!

What Every Job Starts With?



Secure. Comply. Save.

What Every Job Starts With?



Secure. Comply. Save.

1. Access Pumps/Switches

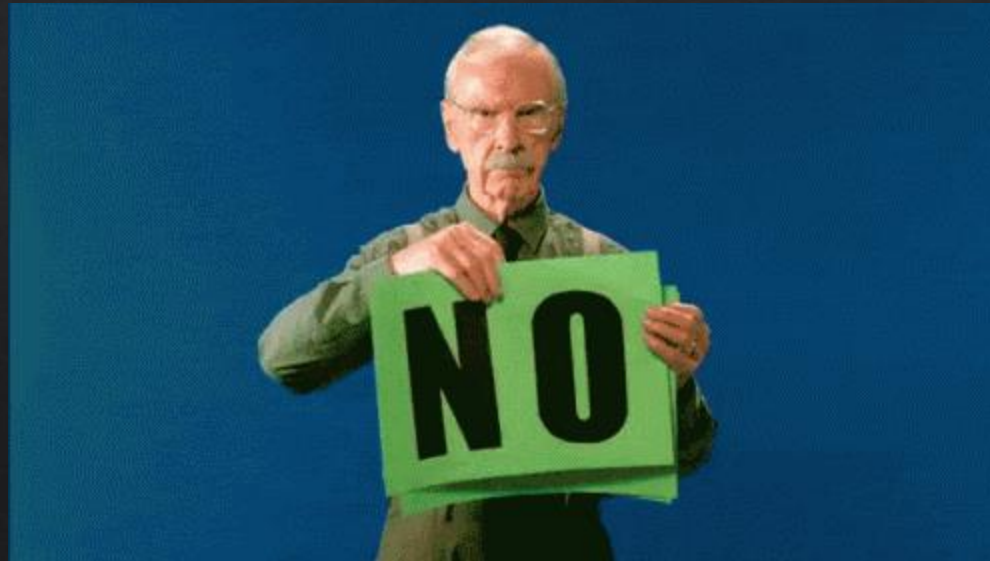
Flags/Goals



1. Access Pumps/Switches
2. Pour white powder into water

Flags/Goals

1. Access Pumps/Switches
2. Pour white powder into water



Secure. Comply. Save.

Flags/Goals

1. Access Pumps/Switches
- ~~2. Pour white powder into water~~
3. Access clean water tanks

Flags/Goals

1. Access Pumps/Switches
- ~~2. Pour white powder into water~~
3. Access clean water tanks
4. Get unescorted access on site

Offsite OSINT

Google Maps & Street View

- 6 foot fences & barbed wire
- Cameras & Lights
- Gate with Intercom
- Bounded by a river
- Found the local ISP

Offsite OSINT



Offsite OSINT



Let's Go In



- Water Facility Daytime
- Wastewater Facility Daytime
- Water Facility Nighttime
- Wastewater Facility Nighttime

Secure. Comply. Save.

WWYD?

Offsite OSINT

Google Maps & Street View

- 6 foot fences & barbed wire
- Cameras & Lights
- Gate with Intercom
- Bounded by a river
- **Found the local ISP**

Daytime Access



Let's Walk Right In

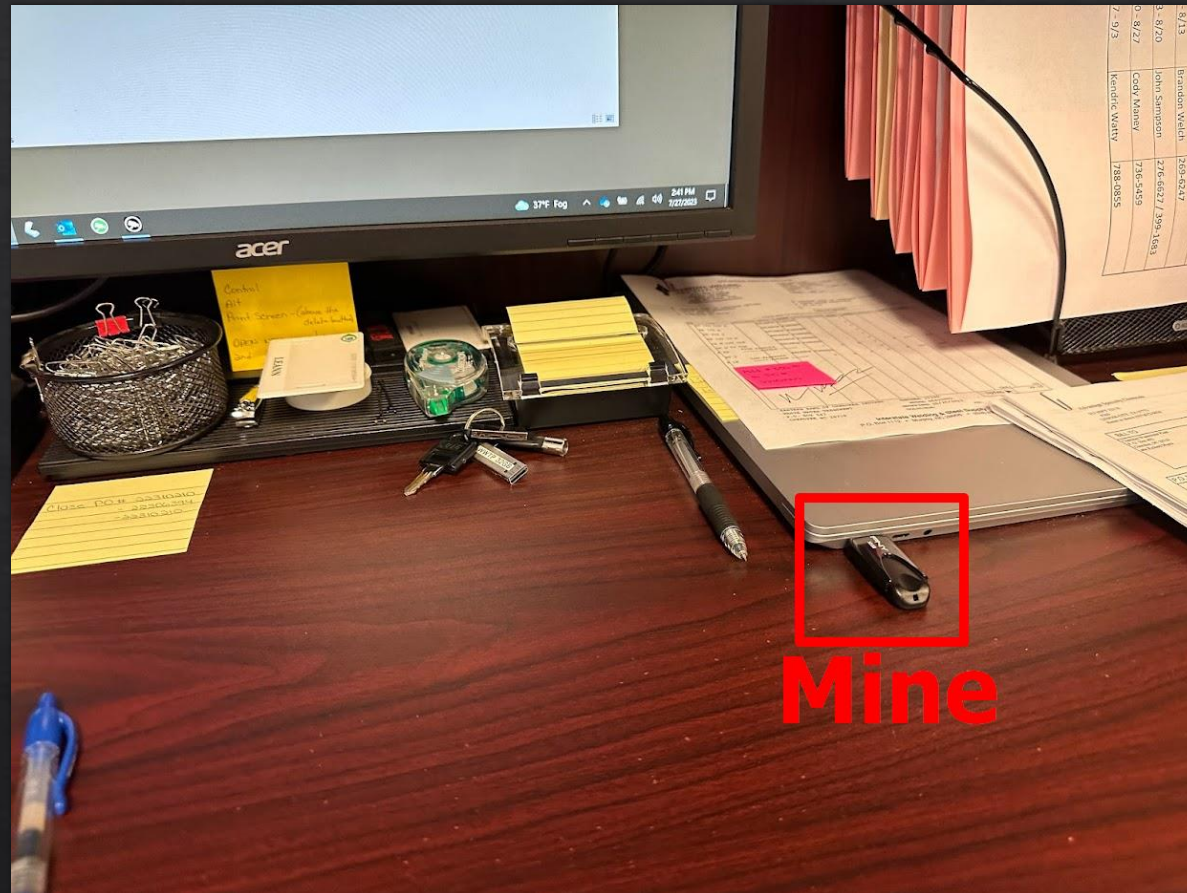
Secure. Comply. Save.

Dress the Part



Secure. Comply. Save.

Can I Do a Speed Test?



Secure. Comply. Save.

Clean Water Access?



Secure. Comply. Save.

Night Access



No Good Reason to Be There

Secure. Comply. Save.

Night Access Water Facility



Night Access Water Facility



Secure. Comply. Save.

Night Access Wastewater Facility



Two Options for Access



Secure. Comply. Save.

Night Access Wastewater Facility



Two Options for Access



Secure. Comply. Save.

Night Access Wastewater Facility



Secure. Comply. Save.

Night Access Wastewater Facility



Secure. Comply. Save.

Night Access Wastewater Facility



Secure. Comply. Save.

Scope Recap

- ☒ Unescorted access to the facility
- ☒ Get access to clean water tanks
- ☒ Get access to pump switches
- ☒ ~~Steal~~ Reposition a company vehicle

Repositioning a Vehicle



Secure. Comply. Save.

Defense – How To Stop Us



Secure. Comply. Save.

Defense – How To Stop Us

- ◆ Keep the Gates Locked
- ◆ Escort all Access
- ◆ Don't Allow Separation of Guests
- ◆ Keep Computers Locked
- ◆ Don't Allow Speed Tests
- ◆ Validate with the Relevant Department
- ◆ Clean Desk Policy
- ◆ Motion Sensors on Grounds
- ◆ Motion Sensor Lights
- ◆ Monitor Security Cameras
- ◆ Lock Access to PLCs
- ◆ Educate Staff on SCADA Security
- ◆ Validate with the Relevant Department

Defense – How To Stop Us

- ◆ Keep the Gates Locked
- ◆ Escort all Access
- ◆ Don't Allow Separation of Guests
- ◆ Keep Computers Locked
- ◆ Don't Allow Speed Tests
- ◆ Validate with the Relevant Department
- ◆ Motion Sensors on Grounds
- ◆ Motion Sensor Lights
- ◆ Monitor Security Cameras
- ◆ Lock Access to PLCs
- ◆ Educate Staff on SCADA Security
- ◆ Validate with the Relevant Department

Verify and Validate!

Secure. Comply. Save.

What Was the Client's Reaction?



Secure. Comply. Save.

What Was the Client's Reaction?



Secure. Comply. Save.

End

Let's Connect!

- ◆ Patrick Lavery
- ◆ PLavery9 on LinkedIn and Twitter
- ◆ PLavery@CompassCyberGuard.com

Bonus for Q&A



Secure. Comply. Save.

Bonus for Q&A



Secure. Comply. Save.

Bonus for Q&A



Secure. Comply. Save.

Bonus for Q&A



Secure. Comply. Save.