Doors, Cameras, & Mantraps: OH MY!

Version 2.1 All the Content Half the Slides

My methods and experiences as a Physical Security Risk Assessor



Who am I?



- I am Dylan “The Magician”
- Member TOOOL (The Open Organization of Lockpickers) in Orlando
- Former Security Consultant with GoldSky
- Former Instructor at UCF
- Pentester Fortune 500
- Overall Security Enthusiast



What did I do?



- **Explored physical sites with on-prem team**
- **Demonstrated Physical Security exploits**
- **Educated clients on vulnerability mitigation**
- **Had fun with our clients**



The Matrix



I’ve found a vulnerability



Show me

What will this talk cover?



1. **Physical Security Controls**
2. **Key questions I asked clients**
3. **How to educate your clients**
4. **How to learn physical security?**

Physical Security Controls: Doors



What to look for with doors?

- **Exposed hinges can have pins removed**
- **Mismatched strike plates can be exploited**
- **Lever handles can be exploited with tools**
- **Gaps in double doors can be susceptible to attack**







Physical Security Controls: Windows



What to look for with windows?

Is information viewable from outside?

Can windows be opened from outside?

Do windows face sensitive areas?



Bourne Identity

Physical Security Controls: Fencing



- **It's challenging to scale a fence without attracting attention.**
- **A fenced and gated perimeter identifies a clear expectation of limited access.**



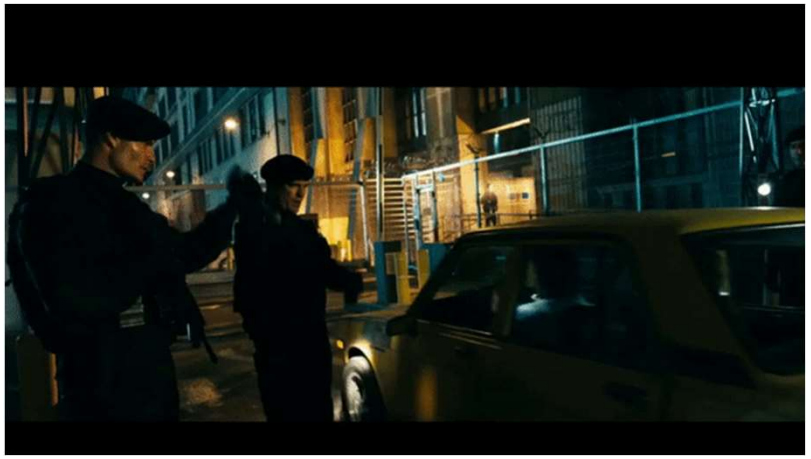
Jurassic Park



Physical Security Controls: Bollards



- **These are reinforced obstacles to prevent the use of vehicles as battering rams to gain physical entry.**



Transformers 3

Physical Security Controls: Mantraps



- **Upon entry a door closes behind a user and a second form of identification is needed to proceed through a second door.**
- **Individuals can be detained in this “holding area”.**
- **Can use multiple authentication forms.**



Physical Security Controls: Cameras

- **Active or Passive monitoring**
- **Great for incident response**
- **Video can be stored for a very long time**
- **Often, they aren't even functional**



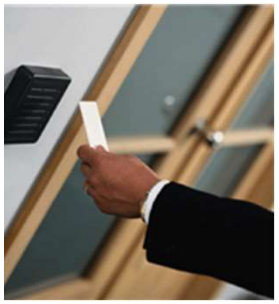




Physical Security Controls: Electronic Access



- **RFID Badges for employee access**
- **PIN Codes for access to privileged areas**
- **Motion sensors for door automation**
- **Biometrics for identification**







Questions I asked clients: What matters



Key areas of importance <u>for your client.</u>

- **Some security gaps may be critical to one business but not to another.**
- **It is important to be efficient with your time.**
- **Knowing what your client needs to secure is important to being a productive security assessor.**

Questions I asked clients: Access from the Perimeter



- **Where are perimeter doors?**
- **Tailgating is a common entry method for attackers.**
- **Some perimeter doors enter sensitive areas.**
- **Frequently used doors will often be targets.**

Questions I asked clients: Guest access policies

- **Is there a robust check-in process?**
- **Will guests need an escort?**
- **Are guest RFID badges dynamic?**
- **Are there policies for guest observation?**
- **Do guests have limited access?**





The Empire Strikes Back

Questions I asked clients:
Do you empower your Employees?

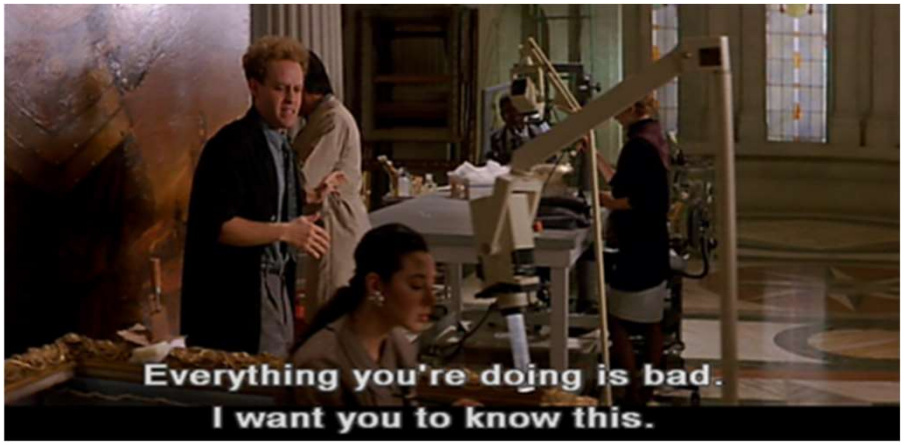


- **Do you gamify security?**
- **Tell employees that company security is job security.**
- **Do you educate your employees about security best practices?**
- **All Employees impact security.**

How to educate clients: Constructive Criticism

- **Empower clients to come to conclusions**
- **Negative approaches toward teach backs hinders the client relationship**





How to educate clients: Demonstrations & Solutions

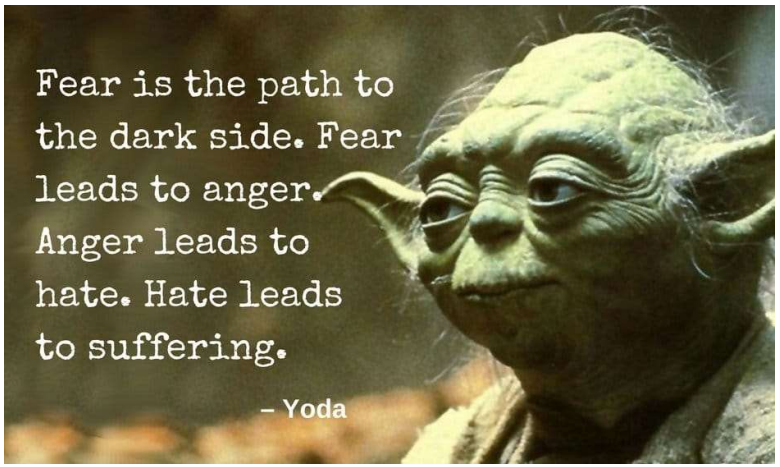


- **Demonstrate Physical Vulnerabilities**
- **Seeing is believing**
- **People get excited about security**
- **Understanding attacks helps defenders**
- **This happens to be the most fun part of the job**

How to educate clients: Avoid Fear, Uncertainty, & Doubt



- **Questions that are accusatory damage the client relationship**
- **Show confidence that issues can be resolved**
- **EXPLAIN don't TELL**



How to educate clients: Provide a means for clients to contact you.



- **Provide a direct e-mail**
- **If provided to you a direct company phone line**
- **Set expectations for when you can be reached**

How to learn PhysSec: Podcasts, YouTube, & Udemy



- **Lockpicking Lawyer –** my favorite YouTube Channel
- **Darknet Diaries –** my favorite Podcast
- **Mike Meyers –** My favorite Udemy Instructor
- **Please take time to find content that speaks to you and that you enjoy.**

How to learn PhysSec: RTFM



- **Dale Carnegie–** How to Win Friends & Influence People
- **Practical Lock Picking –** Deviant Ollam
- **The Art of Deception –** Kevin Mitnick
- **What Every Body is Saying –** Joe Navarro
- **ExamCram**

How to learn PhysSec: Approach Professionals





Deviant Ollam



Ean Meyer



Jayson Street

How to learn PhysSec: Take Guided Courses





Karate Kid

Red Team Alliance

OffSec

SANS

Check with your local colleges for continuing education programs.

How to learn PhysSec: Attend Local Meetups



- **Meet other people in the community**
- **Get hands on experience picking locks**
- **Talk to like minded people**
- **Contact potential employers**
- **Join groups that encompass your interests**

How to learn PhysSec



The Open Organisation Of Lockpickers

Ann Arbor | San Francisco | Boston | Chicago |Colorado Springs | Washington DC | Detroit | Des Moines | Jacksonville | Kansas City | Baltimore | Montreal | New Jersey | New York | Orlando | Ottowa | Portland | Philadelphia | Pheonix | Rochester | Toronto | Las Vegas | Bethesda | Fairfax | Salt Lake City | San Marcos | Houston | Raleigh | Burbank | Seattle

Special thanks...



- Family & Friends
- Orlando Hacker Folks
- TOOOL for educating myself and the public
- Goldsky Security for experiences
- The BSides LPV for letting me speak
- Hacker community at large
  - HACK ALL THE THINGS

Please reach out with questions?

Please contact me if you want to learn anything in more detail this was a lot of info.



dylan@themagician.tech

@31337magician

LinkedIn.com/Dylan-baklor