
ARMY OF DARKNESS
cuter than expected, actually
ICANHASCHEEZBURGER.COM BY

Steal Everything, Kill Everyone, Cause Total Financial Ruin!

(or how I walked in & Misbehaved!)

Jayson E. Street, C|EH, CISSP,
GSEC, GCIH, C|IH,
IEM, IAM, ETC…

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Let go of my EGO

Who Am I?

@jaysonstreet

Let go of my EGO

Who Am I?

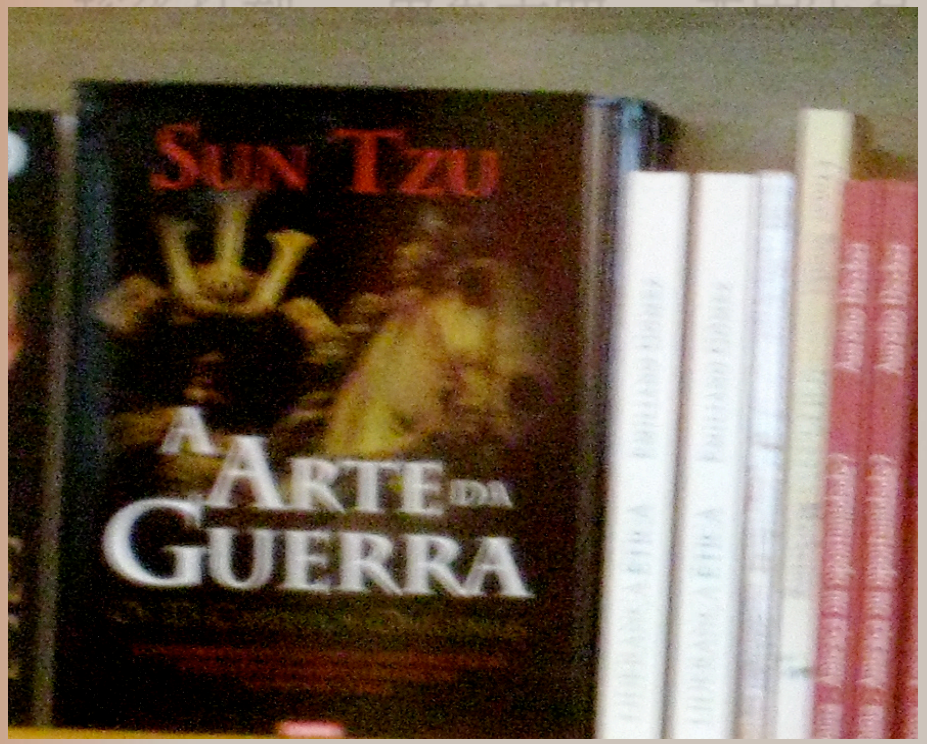
@jaysonstreet

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

Hacker/Social Engineer

INFOSEC talk = slide like this ;-)

- Sun Wu (Tzu) “Ping-fa”(The Art of War)
- “…deception. Hence, ……”



Contents

- INTRO
- 1. Fact
- 2. Rules
- 3. Outcomes
- Outcome 1.
- Outcome 2.
- Outcome 3.
- Conclusions and or Discussions

1. FACT = I’m getting in . and !

1. FACT = I’m getting in . and !

----- Forwarded Message ----
From: Jayson Street <badguy@badstuff.com>
Sent: Mon, February 14, 2011 12:18:22 AM
Subject: Fw: ongoing issues at <Victim CO>

Jayson

As you can tell from this email <Collateral owner> is not very happy and would like this resolved quickly. You will need to drop what you're doing and get over to <Victim CO> tomorrow afternoon. If you have any questions contact me or the person at the location at the number below. Do a good job there will be a lot of eyes on this project. Make sure to keep your presence quite and low key. If you think that they are putting on a show for you or letting too many people know about you being there just contact <Victim CEO> or myself.

Thanks,
<Collateral CIO>

----- Forwarded Message ----
From: <redact> <<redact>@<redact>.com>
To:<redact> <<redact>@<redact>.com>
Cc: <redact> <<redact>@<redact>.com>
Sent: Mon, <redact> 00, 0000 3:46:23 PM

Subject: ongoing issues at <Victim CO.>
Hello <Victim CEO>,

I keep having issues with the network while I am in New York. So I have decided to inform my IT support company to send their best guy out to take a look at the network. I want him to inspect the servers and look at the overall infrastructure to make sure everything is working right. I will also expect him to give us input and recommendations if any improvements need to be done. I don't think I want to get <Victim CIOt> involved in this I want him to come in unannounced to get a real picture on how the network is running. I hope this will be taken care of before I am back in New York.

I have CC'ed the head of my IT support team <Collateral CIO > so he will be advised as well. <Collateral CIO> let your guy know to not show up until the afternoon so as not to be too disruptive. If you have any questions feel free to give <Victim CEO> a call at 212-<redact>

<Collateral owner>

2. Rules =

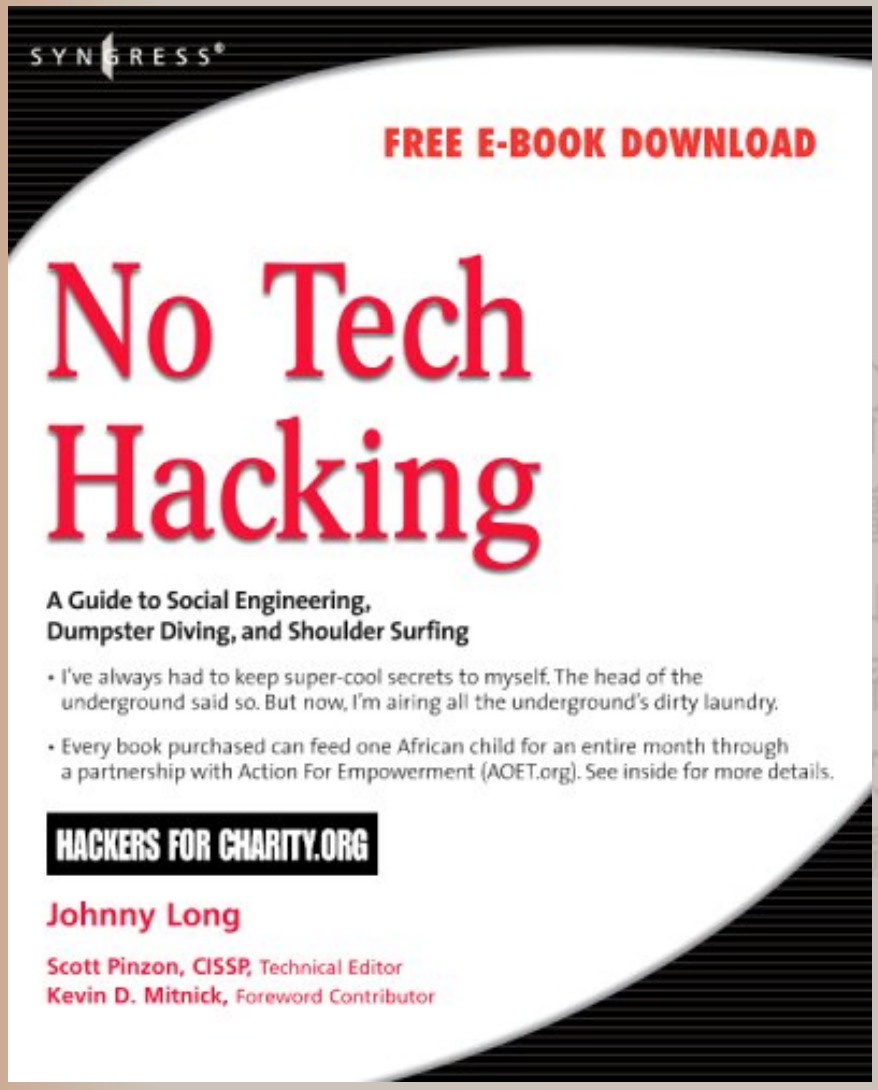
“I aim to misbehave.”

“Let’s go be bad guys.”

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计
走为

3. Outcomes = I’m this guy

3. Outcomes = Also proper credit is due my Sensei



Management is reactive not Proactive

- **“The best way to get management excited about a disaster plan is to burn down the building across the street.”**
- Dan Erwin, Security Officer, Dow Chemical Co. -2008

1. Steal Everything

1. Steal Everything

1. Steal Everything

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计
走为

1. Steal Everything

1. Steal Everything

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

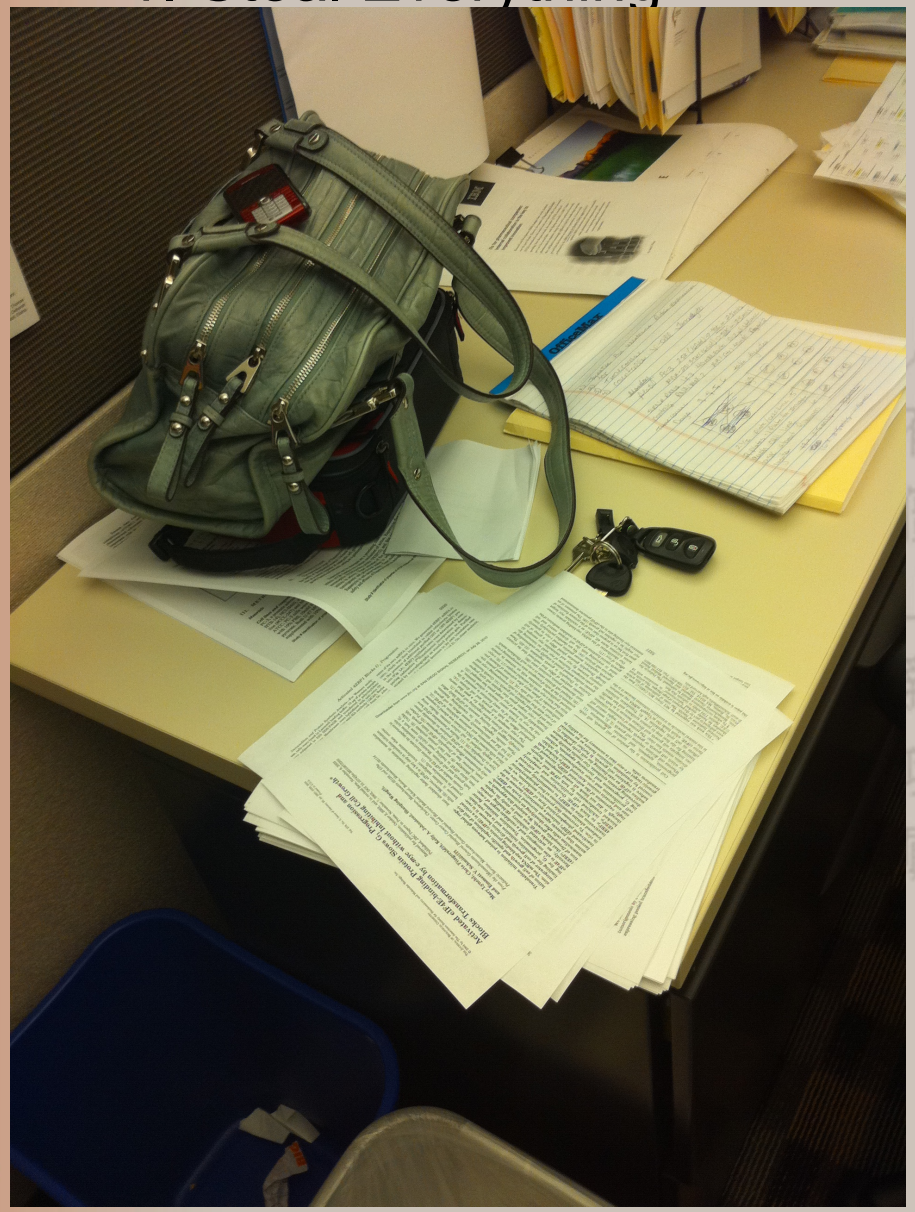
1. Steal Everything

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计

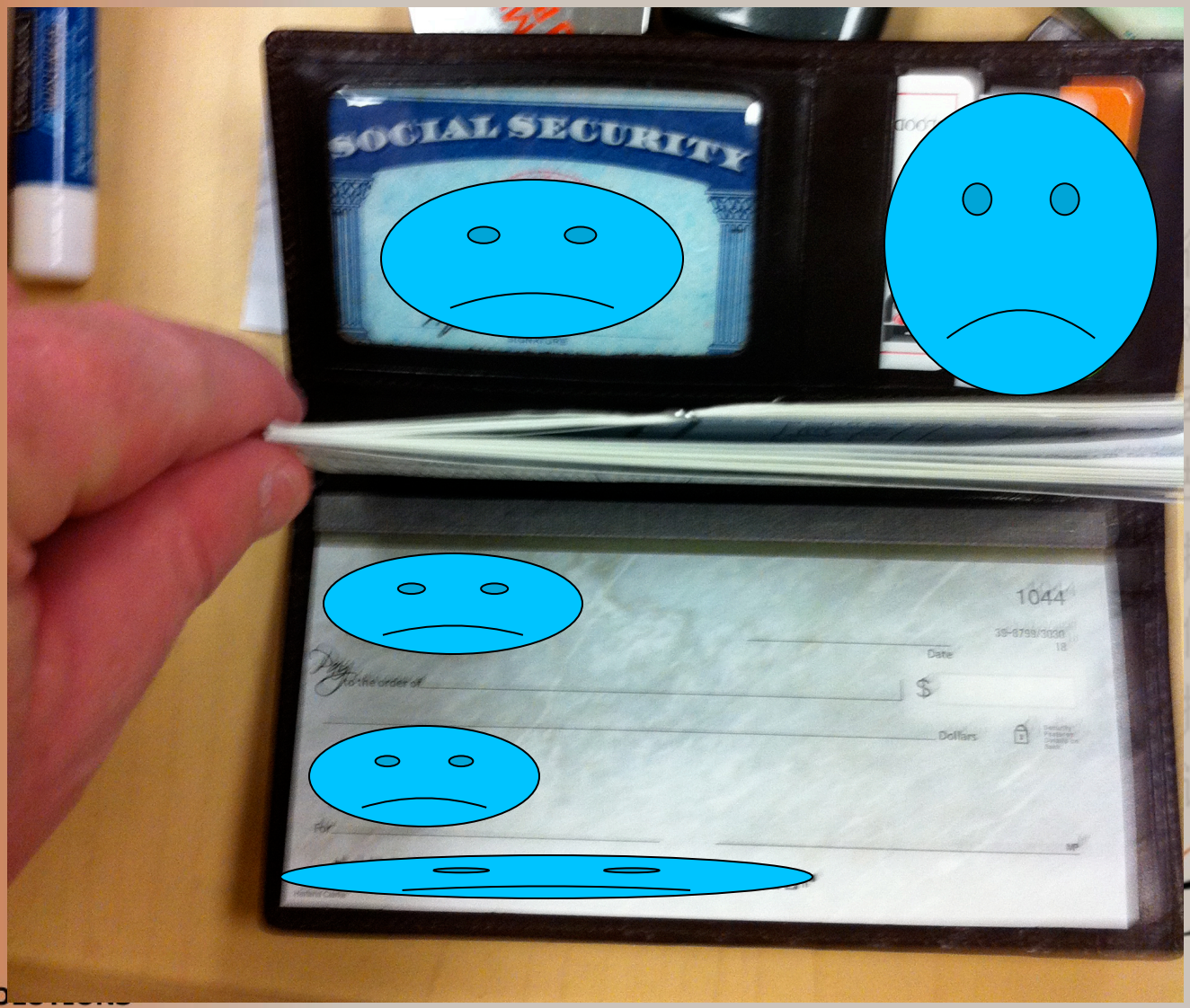
1. Steal Everything

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计

1. Steal Everything



1. Steal Everything



1. Steal Everything

Countermeasures of theft

1. Lock your desk and door when ever you leave (even for a short time).
   Do not leave your wallet, purse, credit cards, cash, checkbook, or other valuables in the open.

2. Never prop open exterior doors. If you see a door propped, close it.

3. Never allow people you do not know to “tailgate” behind you into the building! Every person who is authorized to be in your building should have either card access or a key. Politely tell them that you cannot allow them in and that they need to contact security

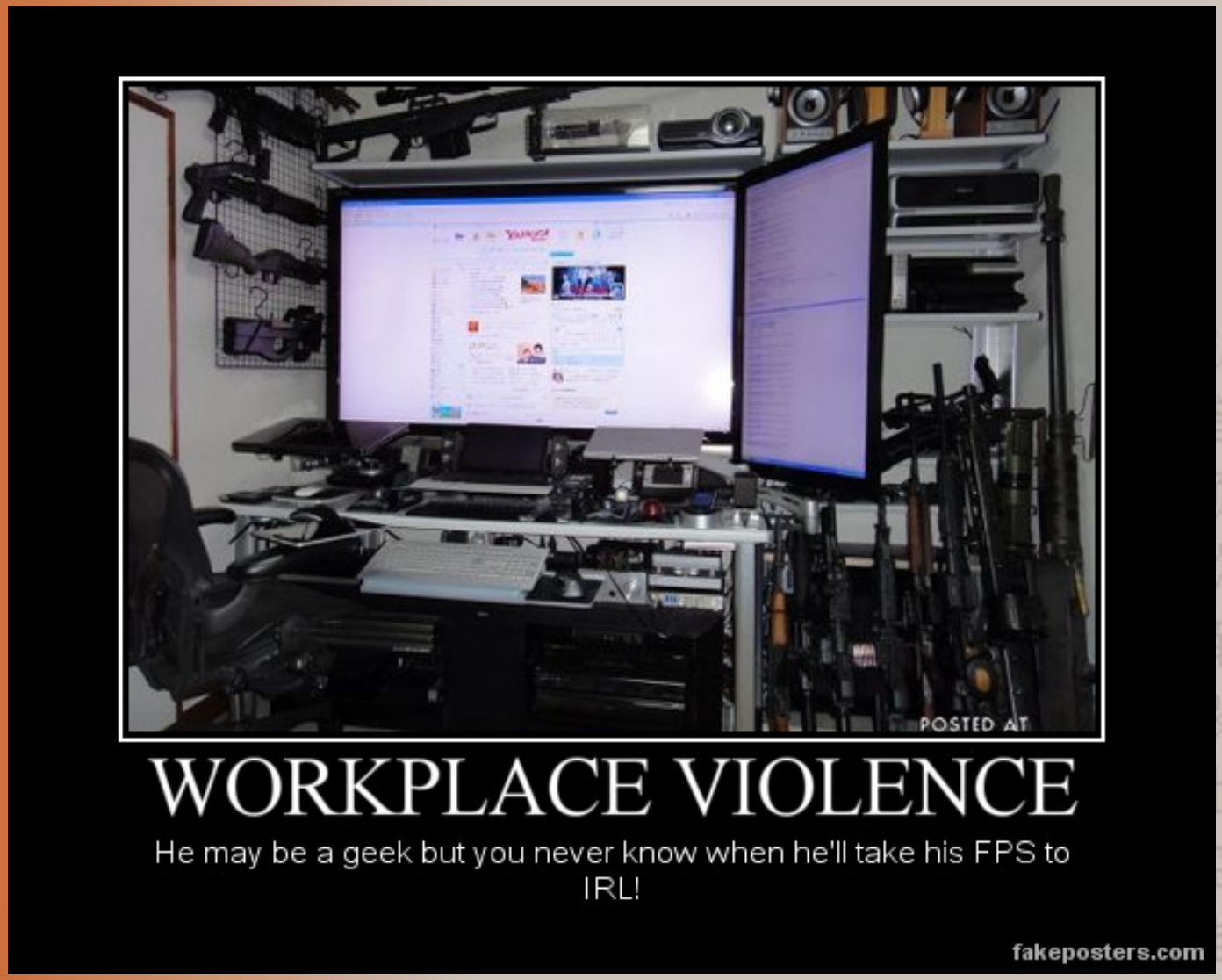
4. Never loan your Company ID card to anyone. If you misplace it, report it to security immediately.

5. Never leave your laptop computer, cell-phone, book bag, purse or other valuables unattended.

6. If you see a suspicious person or someone you don’t believe should be in or around the building call Security or the police immediately.

http://www.usiouxfalls.edu/index.php?option=com_content&task=view&id=366

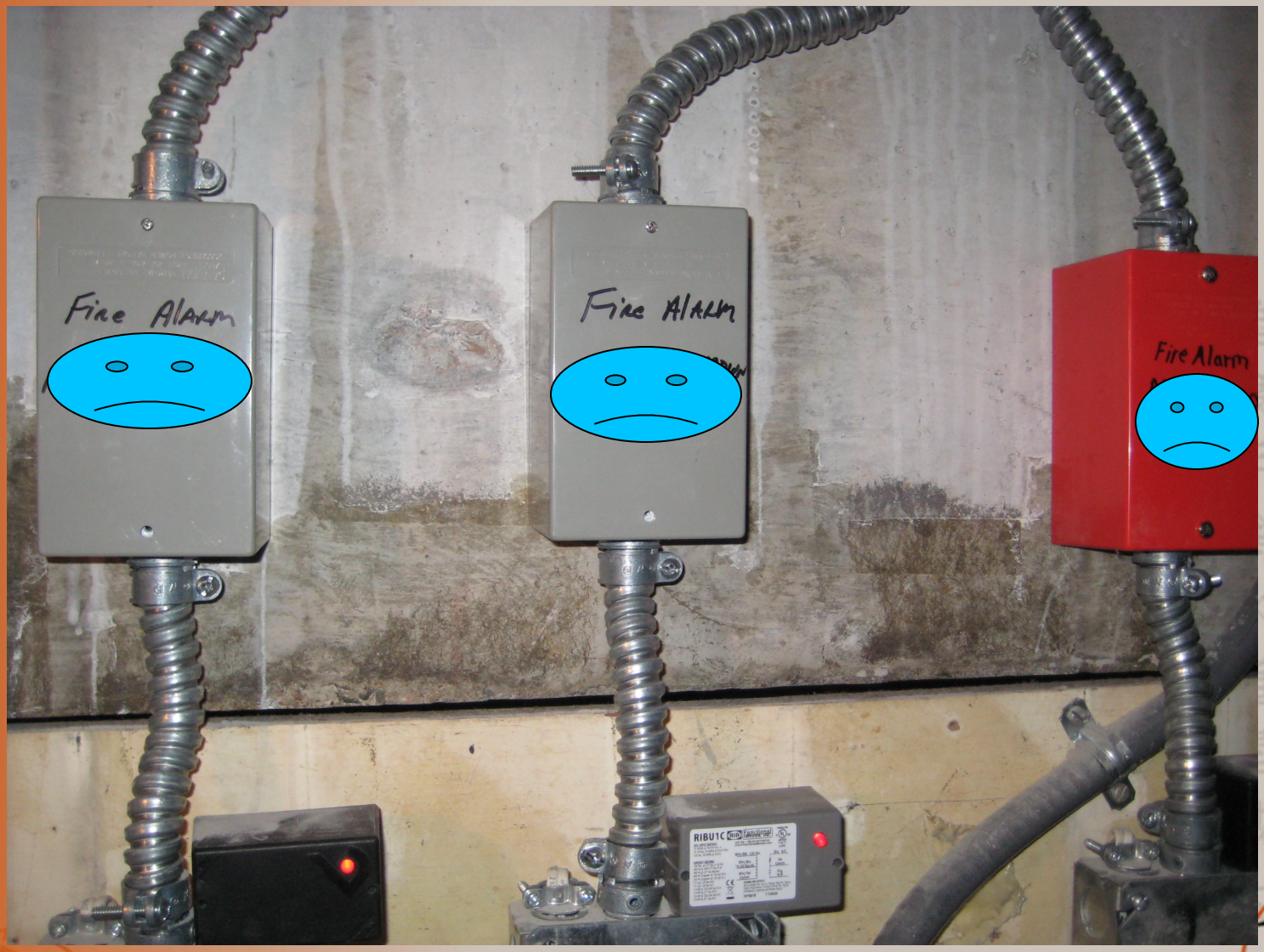
2. Kill Everyone



2. Kill Everyone

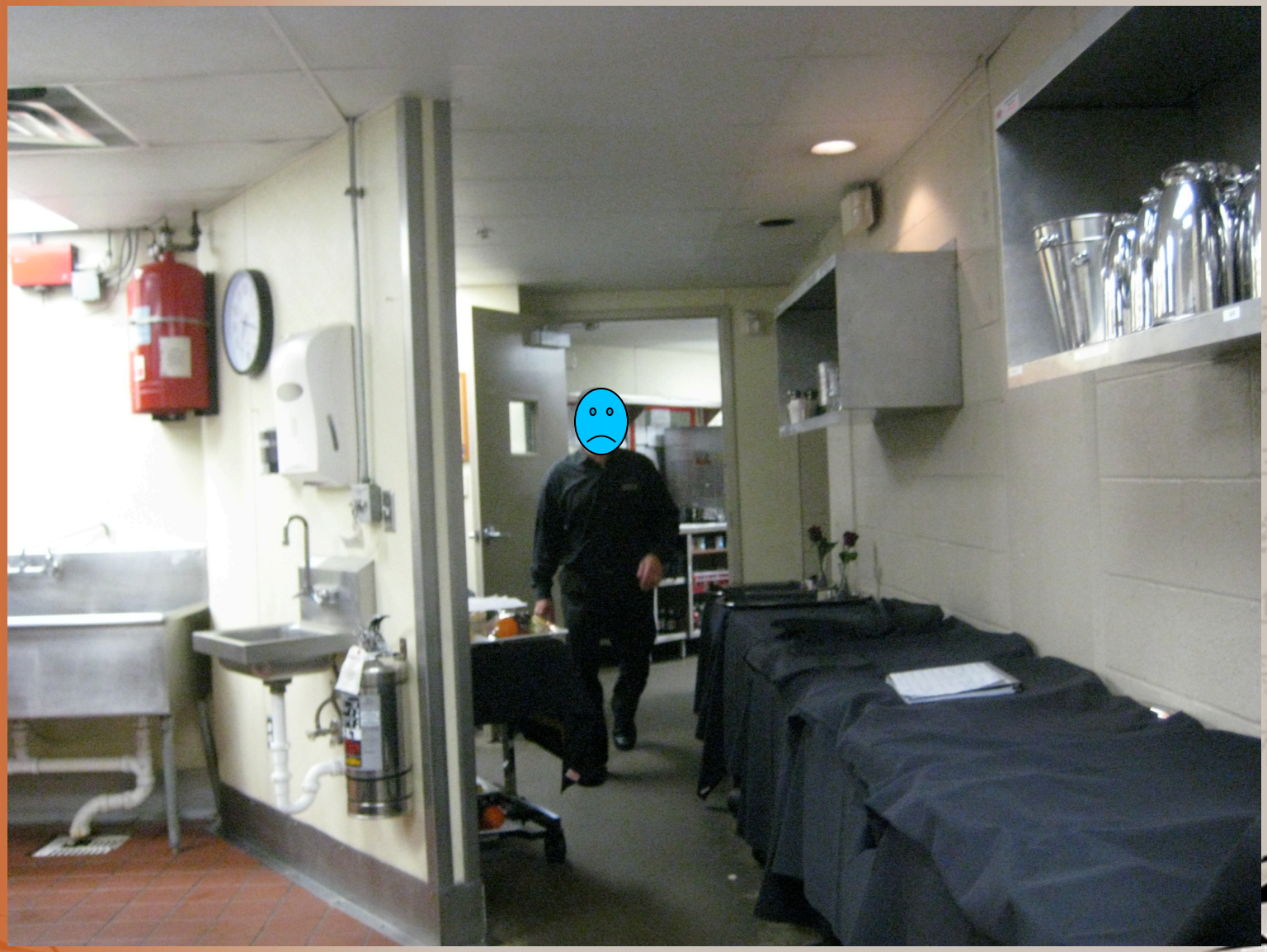
2. Kill Everyone

2. Kill Everyone



2. Kill Everyone

2. Kill Everyone



And just to bring it home…

2. Kill Everyone

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计
树上开花　反客为主　美人计
反间计　苦肉计　连环计
走为

Countermeasures for violence in the workplace

1. Train management and employees to recognize the warning signs of potential workplace violence.

2. When faced with a threat, hire extra security and provide employees with sufficient warning and instructions.

3. Make certain that all employees/victims know that reporting workplace violence, harassment, and/or threats will not affect their job status.

4. Set up a code word that receptionists can use to alert a coworker if a potentially dangerous individual arrives at the reception area.

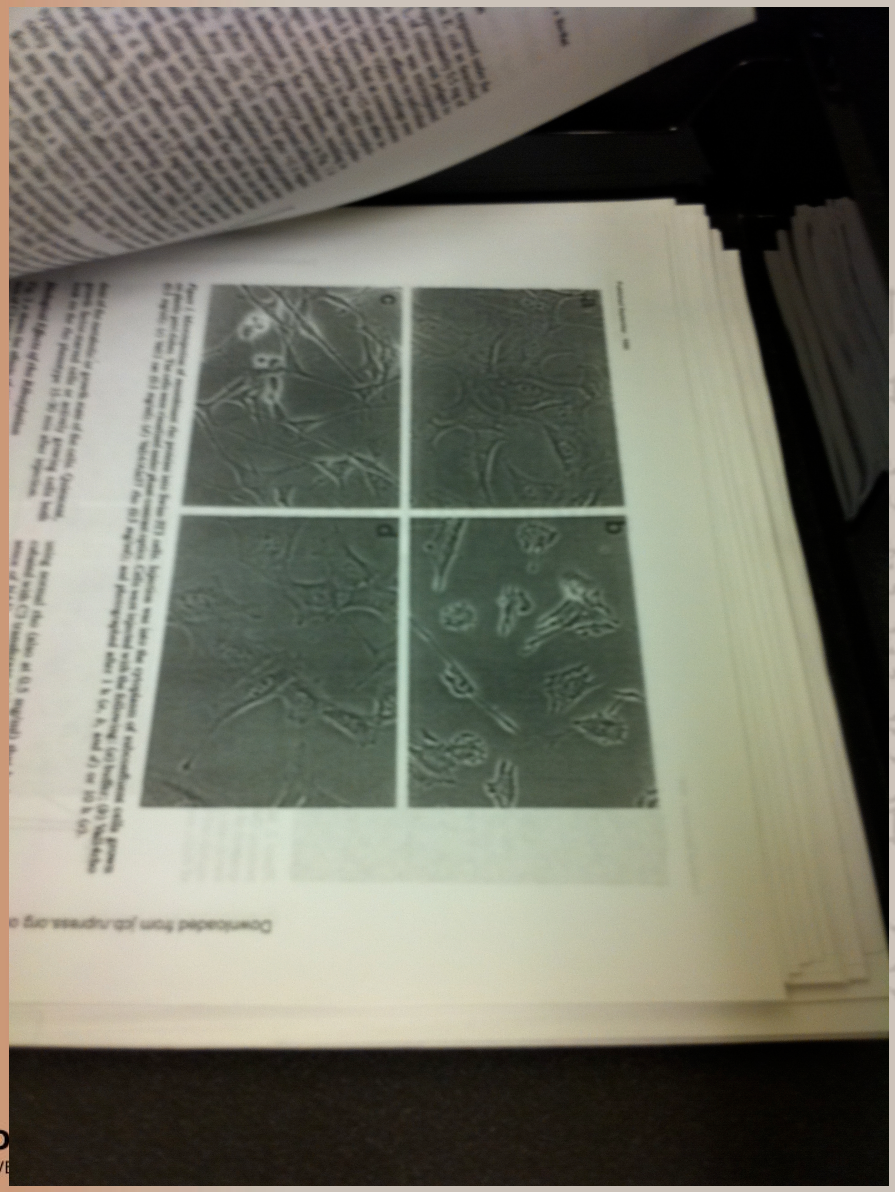
5. Conduct regular training sessions to teach managers and supervisors how to recognize the warning signs of violence and minimize potentially violent situations in the workplace.

6. Conduct routine safety checks and maintenance of features in and around the workplace, including emergency exits, alarms, security lighting, surveillance cameras, and/or metal detectors.

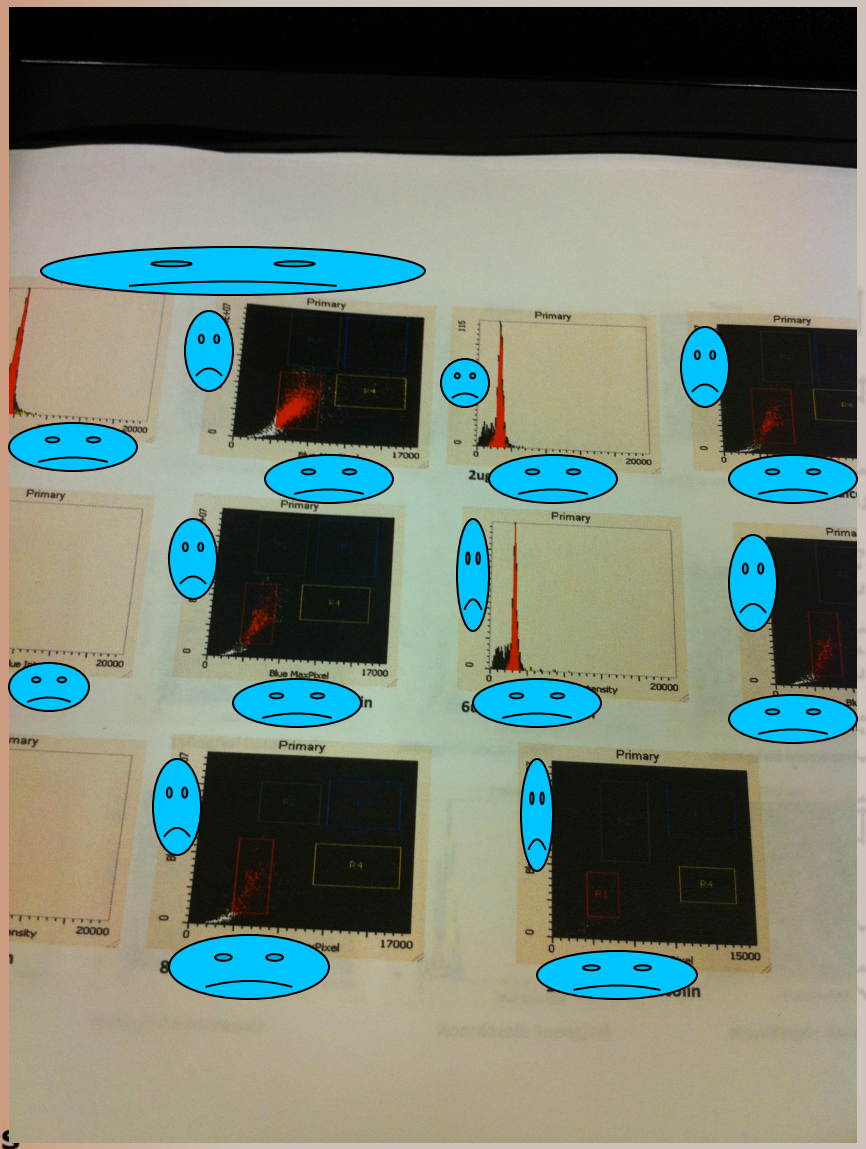
-http://workplaceviolencenews.com/2010/10/04/workplace-violence-prevention-tips-for-employers/

3. Cause total Financial ruin

3. Cause total Financial ruin



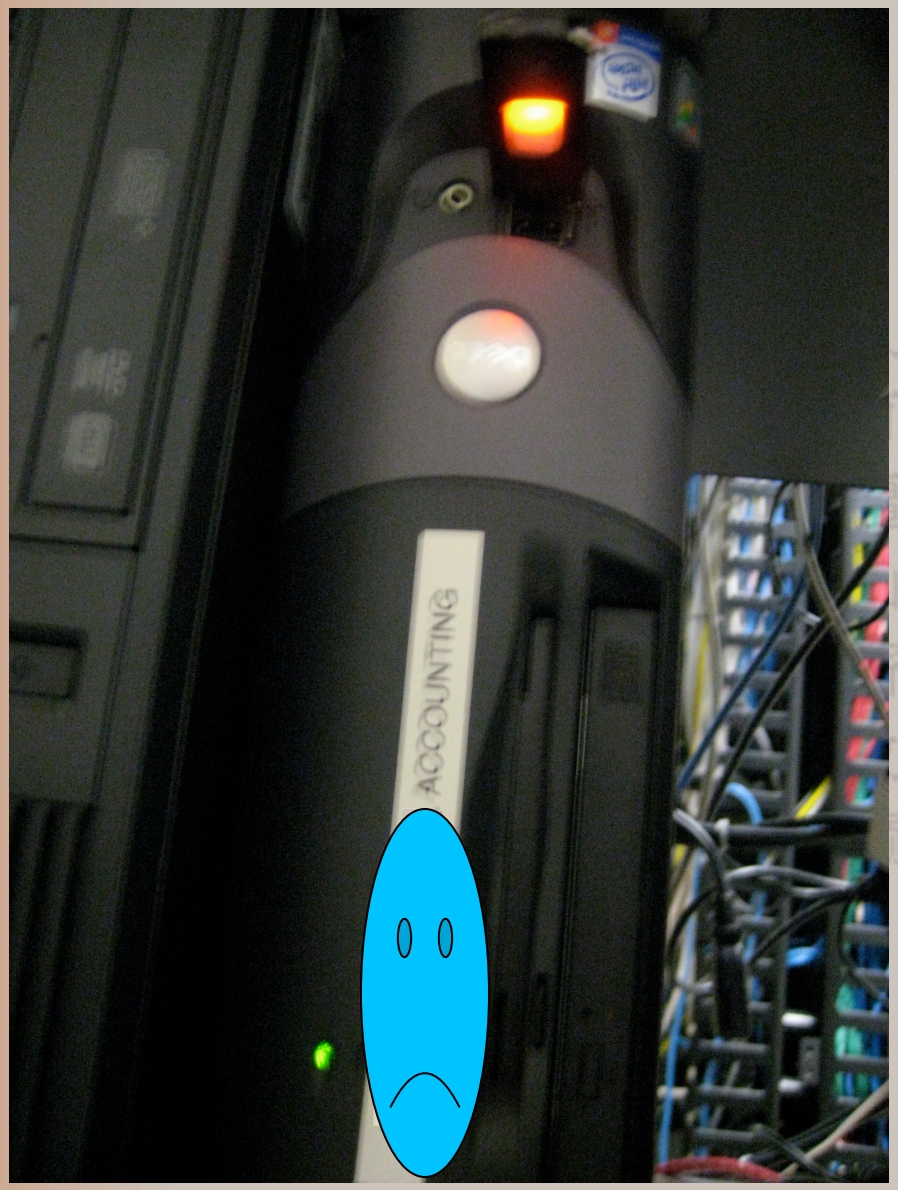
3. Cause total Financial ruin



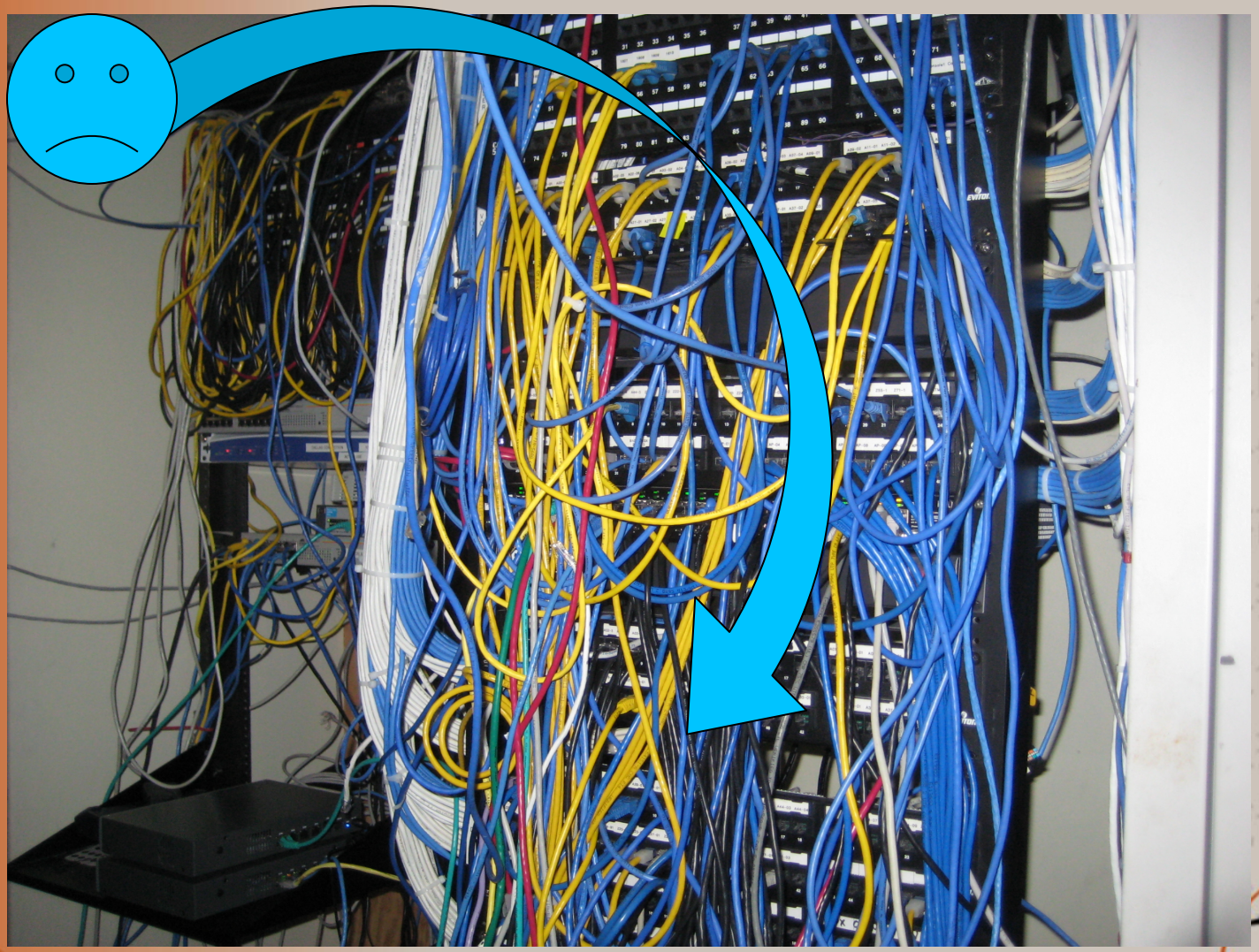
3. Cause total Financial ruin

3. Cause total Financial ruin

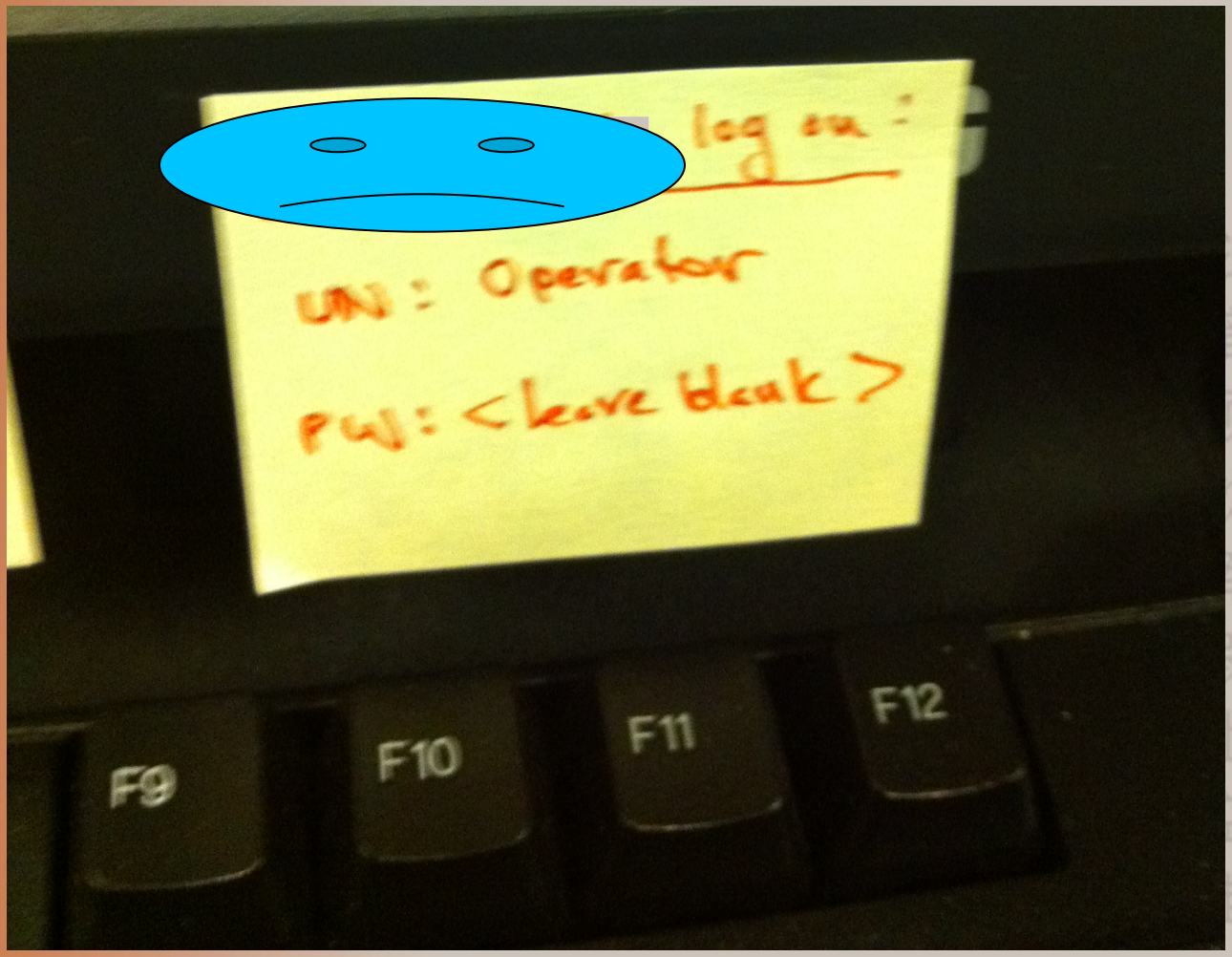
3. Cause total Financial ruin



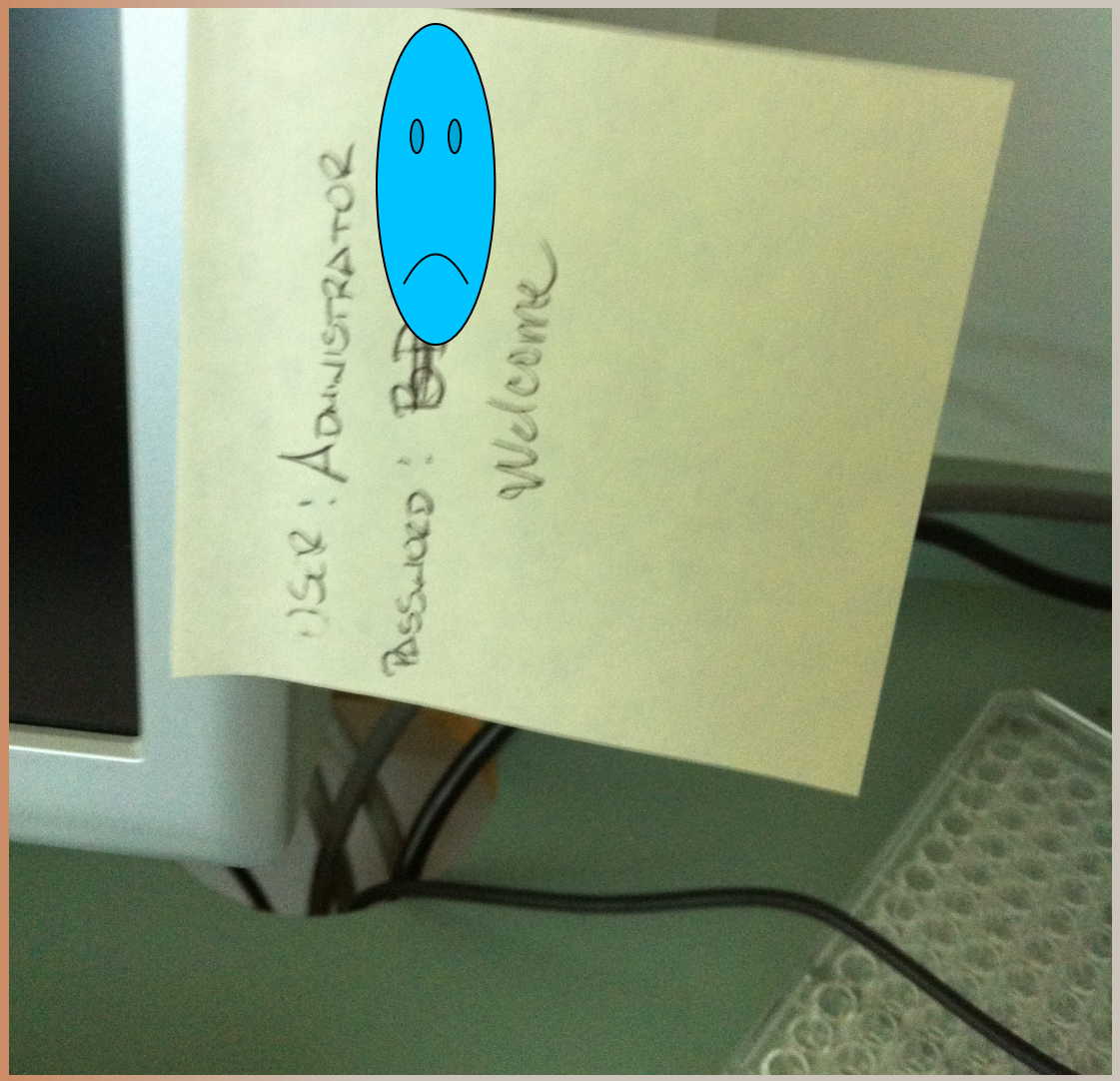
3. Cause total Financial ruin



3. Cause total Financial ruin



3. Cause total Financial ruin



以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计
走为

3. Cause total Financial ruin

以逸待劳
暗渡陈仓
顺手牵羊
欲擒故纵
浑水摸鱼
假道伐虢
上屋抽梯
空城计
走为

STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

3. Cause total Financial ruin

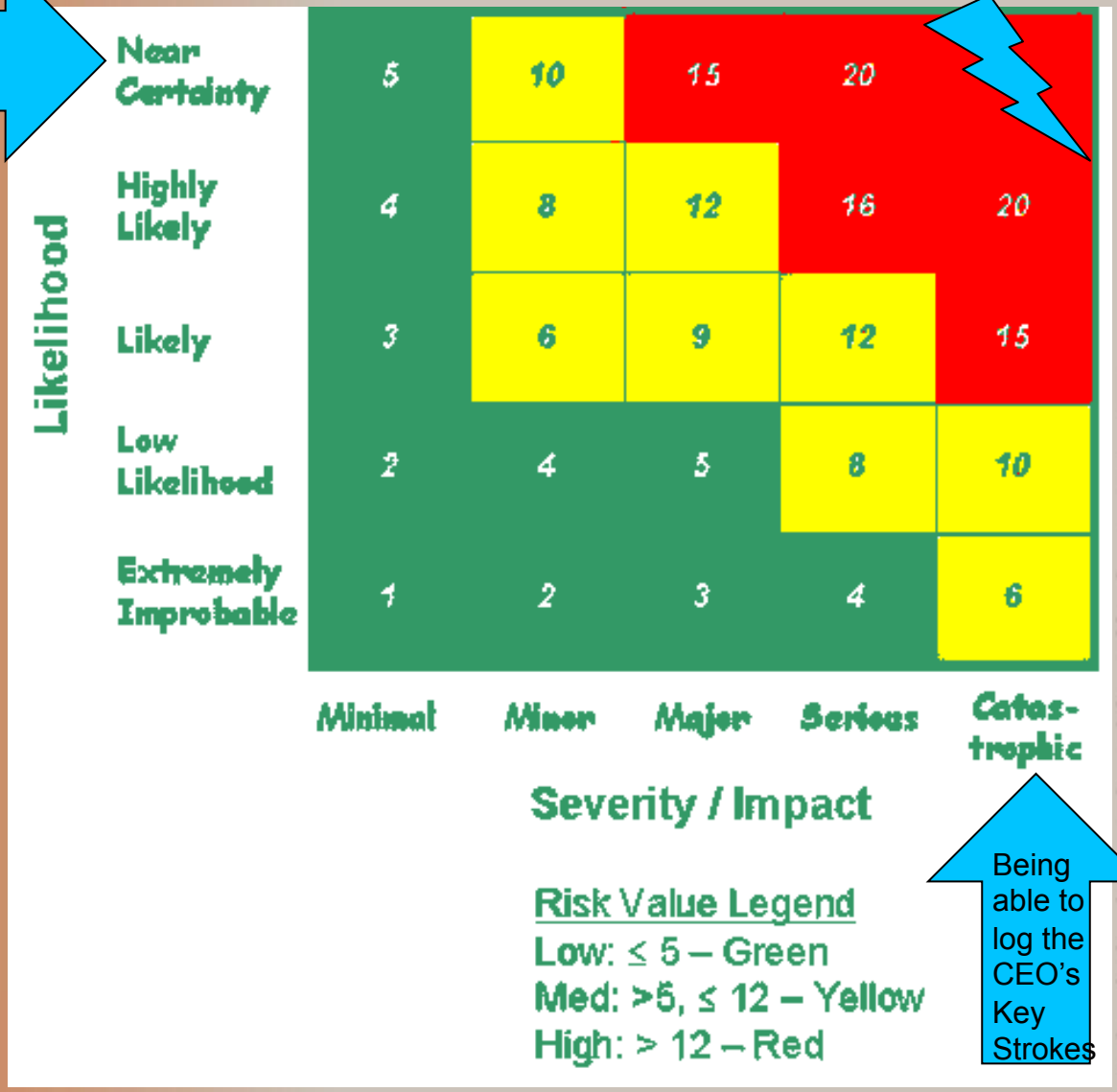
STRATAGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"

3. Cause total Financial ruin

3. Cause total Financial ruin

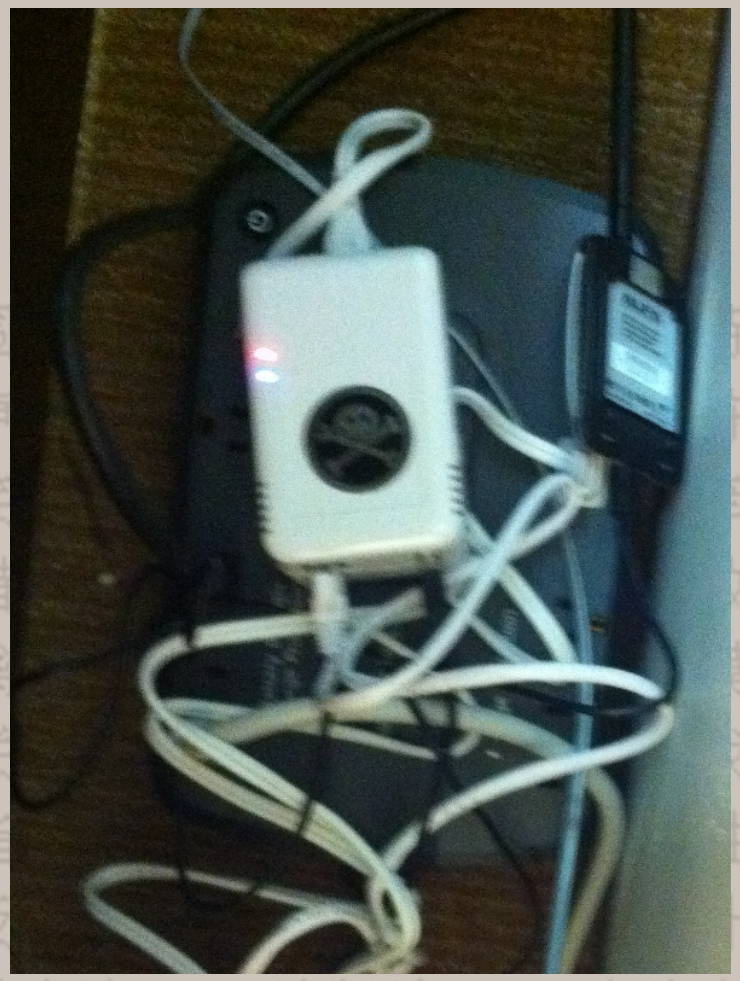
3. Cause total Financial ruin

Available at geek/gadget website



Being able to log the CEO's Key Strokes

3. Cause total Financial ruin



http://pwnieexpress.com/

Countermeasure for Corporate Espionage

1. Since a majority of information stolen is in the physical form, companies should shred all documents before they are discarded

2. Do not print sensitive company information unless it is absolutely necessary. Then immediately place the information in a secure envelope or place until it reaches the intended party. Information lying around on a desk may be easily copied, photographed, or stolen.

3. Secure all necessary printed documents in a locked file cabinet. Keep the cabinets locked when the cabinets are not in use.

4. Companies should invest in technology that prevents documents with sensitive company information from being copied.

5. Companies may set access controls within software indicating authorized parties that are allowed to print specific runs of specific documents. This will prevent individuals from carelessly printing materials which may expose the company to unnecessary risks.

6. Print encryption is another method to protect sensitive company information. When a document is printed, it hides sensitive information in the print fields where the encryption occurs. The information encrypted may only be viewed by individuals who possess the authority to view the information.

http://www.businesssecurity.net/business-espionage/

Okay now what can we do?

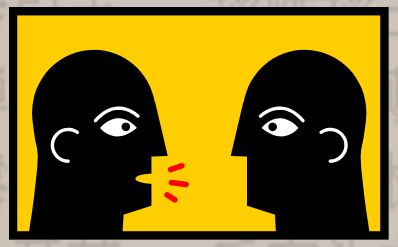
Okay now what can we do?

- Without understanding where the opponent's weaknesses are you cannot borrow their strength to use against them. (Cheng Man Ching)

- http://www.dissectingthehack.com
- http://f0rb1dd3n.com
- http://headhacker.net
- http://www.social-engineer.org/
- http://netragard.com
- http://mjc.me
- http://pwnieexpress.com/
- @jaysonstreet on Twitter

Now let's learn from others

- Discussion and Questions????
- Or several minutes of uncomfortable silence it's your choice.



- This concludes my presentation Thank You

Those Links Again

- http://www.dissectingthehack.com
- http://f0rb1dd3n.com
- http://headhacker.net
- http://www.social-engineer.org/
- http://netragard.com
- http://mjc.me
- http://pwnieexpress.com/

- @jaysonstreet on Twitter