



ARMY OF DARKNESS

cuter than expected, actually

ICANHASCHEEZBURGER.COM BY

STRATEGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"



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...**

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
走为上



Let go of my EGO

Who Am I?



海 劫 火 蛇 玉 壳 桂 花

围 数 声 东 笑 里 借 月 捲 财

反 客 为 主

美 人 计

苦 肉 计

连 环 计

@jaysonstreet



Let go of my EGO

Who Am I?



反客为主
苦肉计

美人计
连环计

空城计
走为上

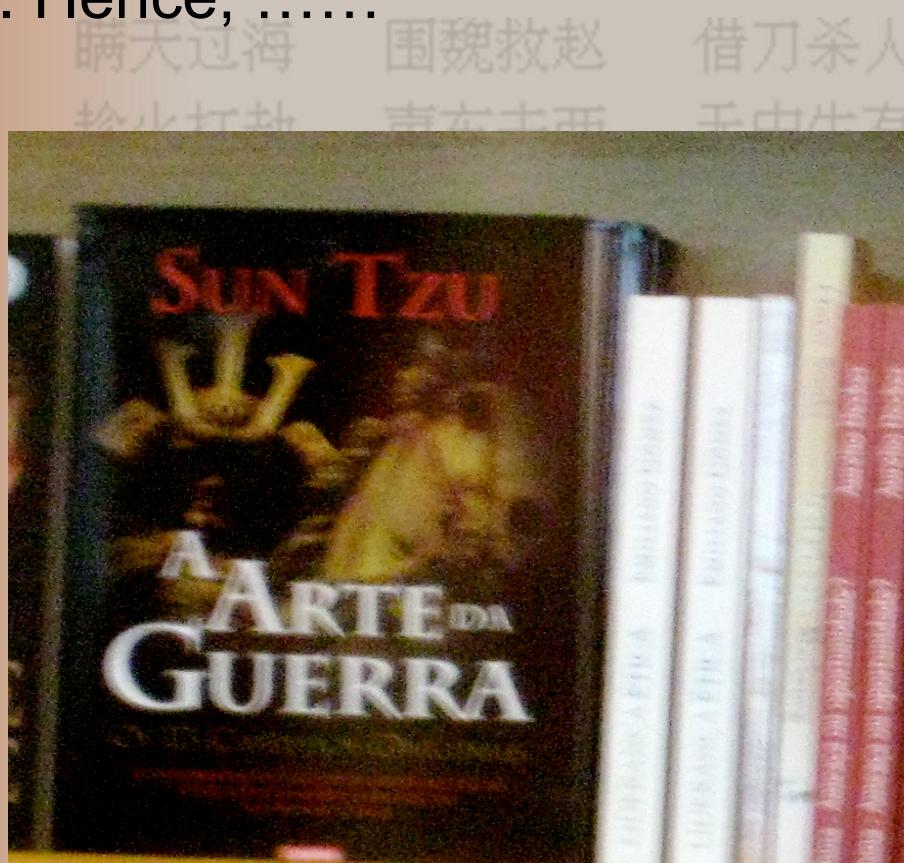
@jaysonstreet



Hacker/Social Engineer

INFOSEC talk = slide like this ;-)

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



瞒天过海 围魏救赵 借刀杀人 以逸待劳
暗渡陈仓 顺手牵羊 欲擒故纵 浑水摸鱼
趁火打劫 南辕北辙 釜中生火 假道伐虢
上屋抽梯 空城计 走为上



Contents

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

瞒天过海

趁火打劫

隔岸观火

打草惊蛇

抛砖引玉

金蝉脱壳

偷梁换柱

树上开花

反间计

围魏救赵

声东击西

笑里藏刀

借尸还魂

擒贼擒王

关门捉贼

指桑骂槐

反客为主

苦肉计

借刀杀人

无中生有

李代桃僵

调虎离山

釜底抽薪

远交近攻

假痴不癫

美人计

连环计

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

走为上计



1. FACT = I'm getting in . and !

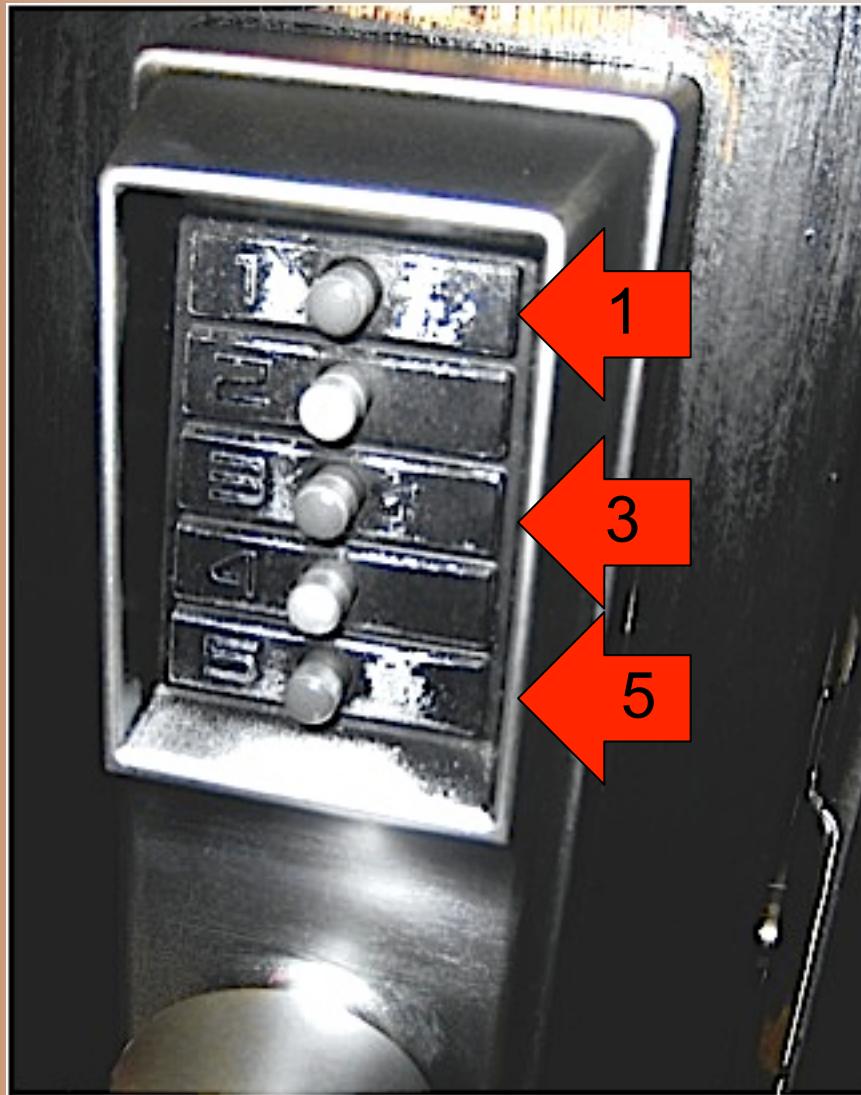


杀人
生有
桃僵
离山
抽薪
近攻
不癲
计
计

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
走为上



1. FACT = I'm getting in . and !



杀人
生有
桃僵
离山
抽薪
近攻
不癫
计计

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
走为上



----- 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 CIO> 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>

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
走为上





逸待劳
渡陈仓
手牵羊
擒故纵
摸鱼
伐虢
屋抽梯
空城计



STRATEGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"



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
走为上



3. Outcomes = I'm this guy



反间计

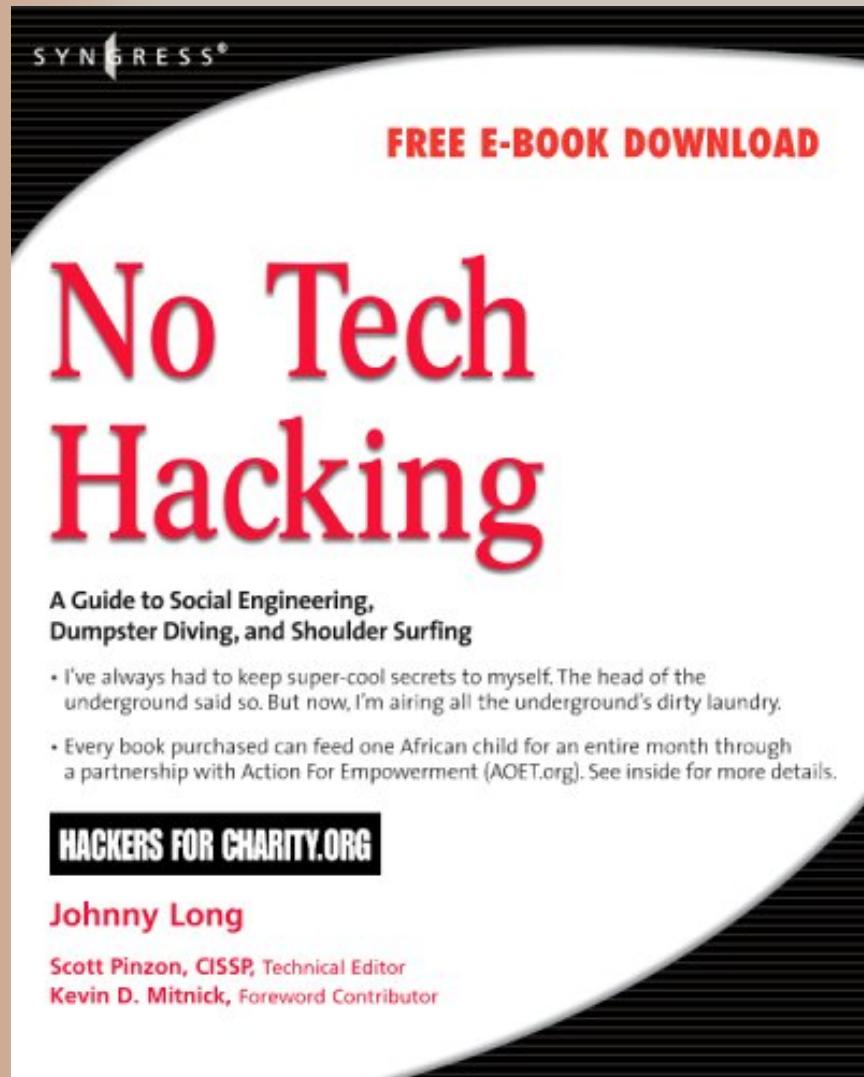
苦肉计

连环计

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
走为上计



3. Outcomes = Also proper credit is due my Sensei



The image shows the front cover of a book titled "No Tech Hacking". The title is prominently displayed in large red letters. Below the title, the subtitle reads "A Guide to Social Engineering, Dumpster Diving, and Shoulder Surfing". The book is published by Syngress, as indicated by the logo at the top left. A red banner across the top right says "FREE E-BOOK DOWNLOAD". At the bottom, there is a black bar with the text "HACKERS FOR CHARITY.ORG" in white. The author's name, "Johnny Long", is printed below the subtitle. Below the author's name, it lists "Scott Pinzon, CISSP, Technical Editor" and "Kevin D. Mitnick, Foreword Contributor".

<http://www.lares.com/>

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
走为上



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

瞒天过海	围魏救赵	借刀杀人	以逸待劳
暗渡陈仓	无中生有	顺手牵羊	隔岸观火
顺手牵羊	李代桃僵	欲擒故纵	打草惊蛇
欲擒故纵	调虎离山	浑水摸鱼	抛砖引玉
浑水摸鱼	釜底抽薪	假道伐虢	金蝉脱壳
假道伐虢	远交近攻	上屋抽梯	偷梁换柱
上屋抽梯	假痴不癫	空城计	树上开花
空城计	美人计	走为上计	反间计
走为上计	连环计		



1. Steal Everything



S U C K E R S

Even baby ducks know how to spot them!



1. Steal Everything



逸待劳
渡陈仓
手牵羊
擒故纵
水摸鱼
道伐虢
屋抽梯
城计
为



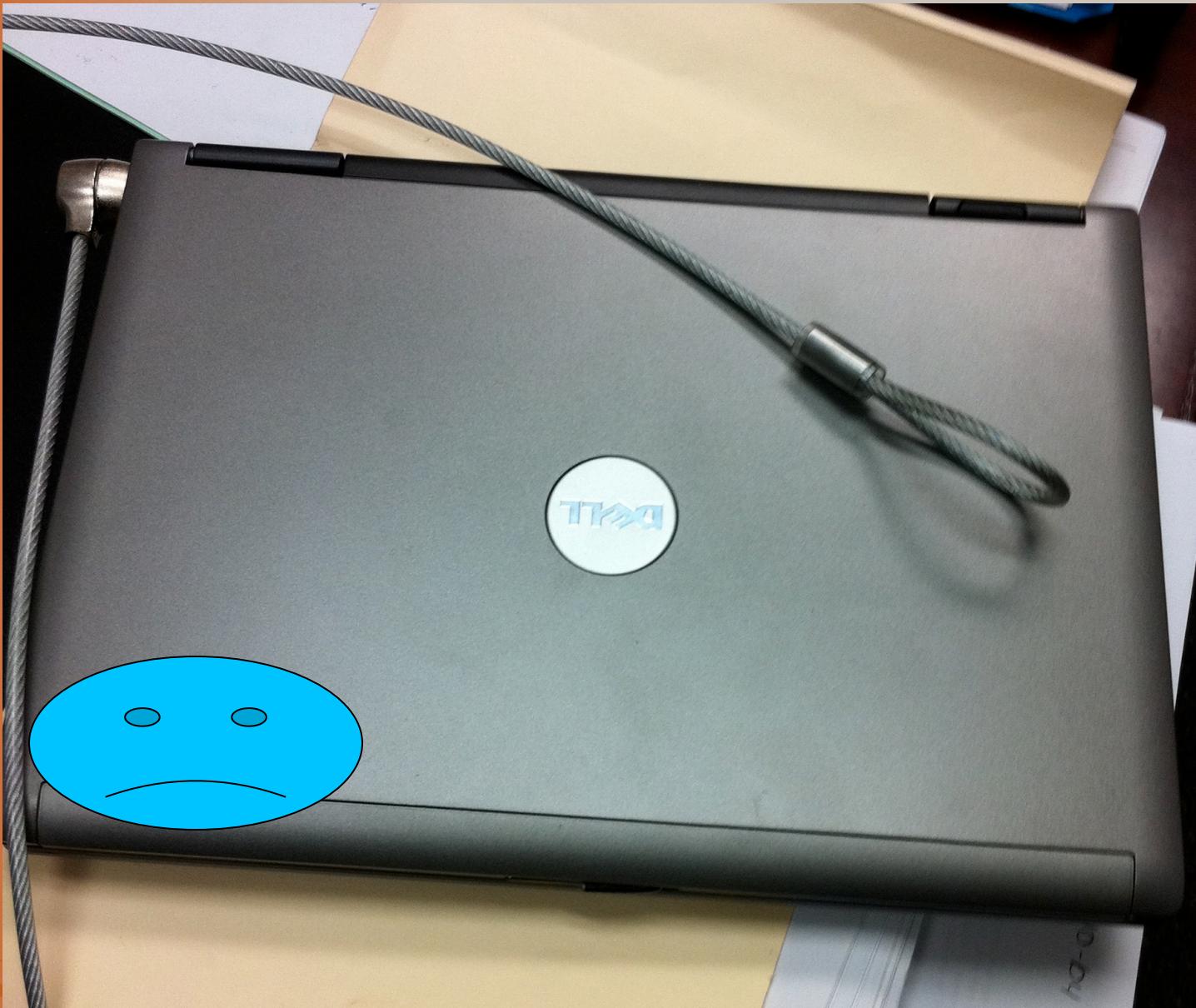
1. Steal Everything



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
走为上



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
走为上



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
走为上



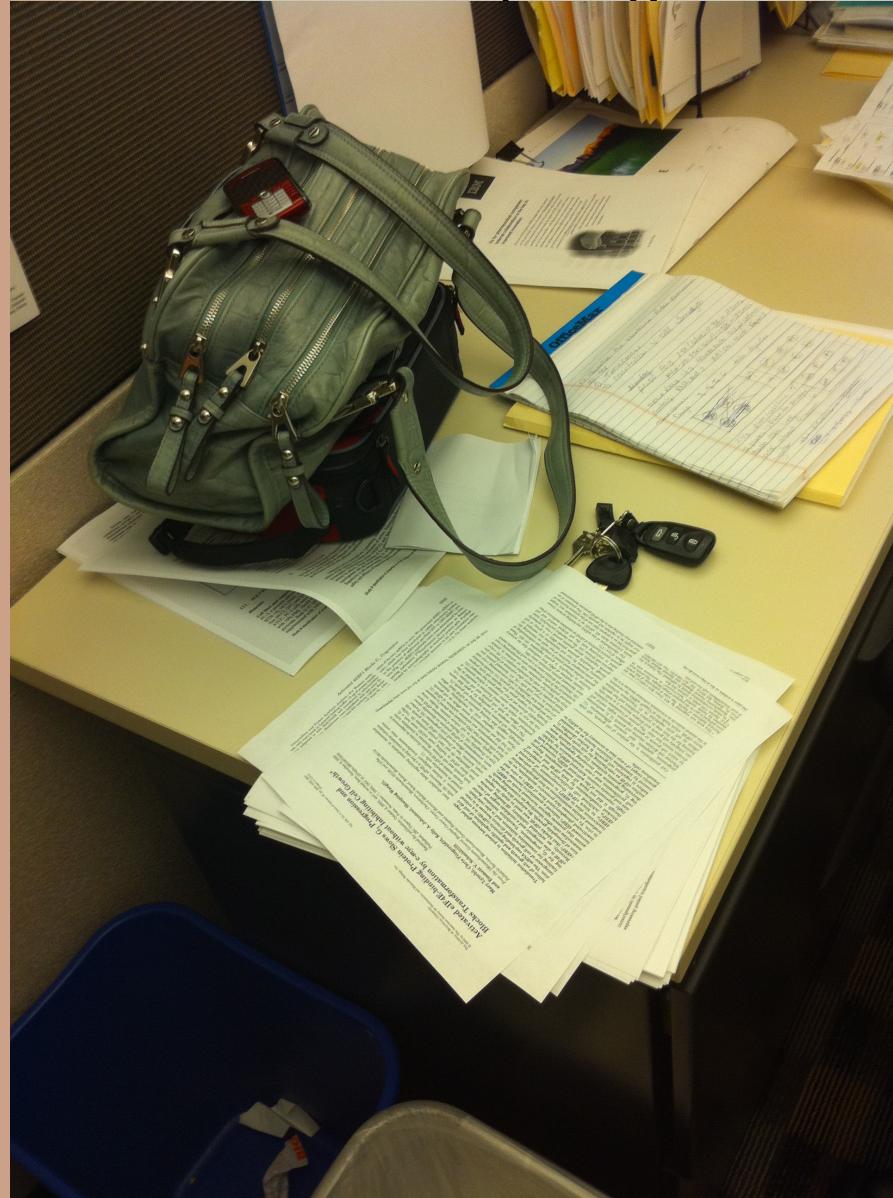
1. Steal Everything



人有
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
走为上



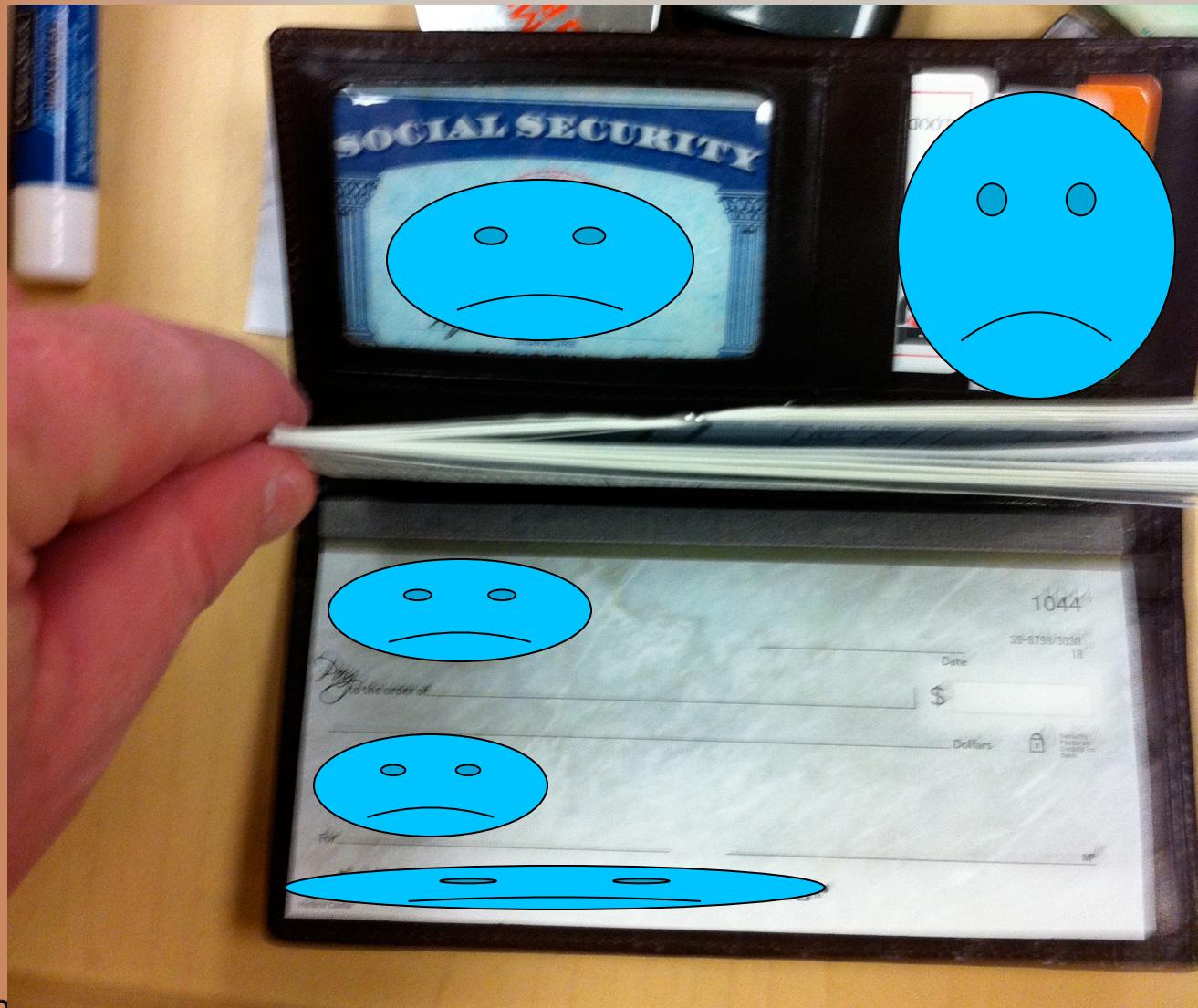
1. Steal Everything



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
走为上



1. Steal Everything



待劳
陈仓
牵羊
纵故
模鱼
伐虢
抽梯
计



1. Steal Everything



逸待劳
渡陈仓
手牵羊
擒故纵
水摸鱼
道伐虢
屋抽梯
城计
为也



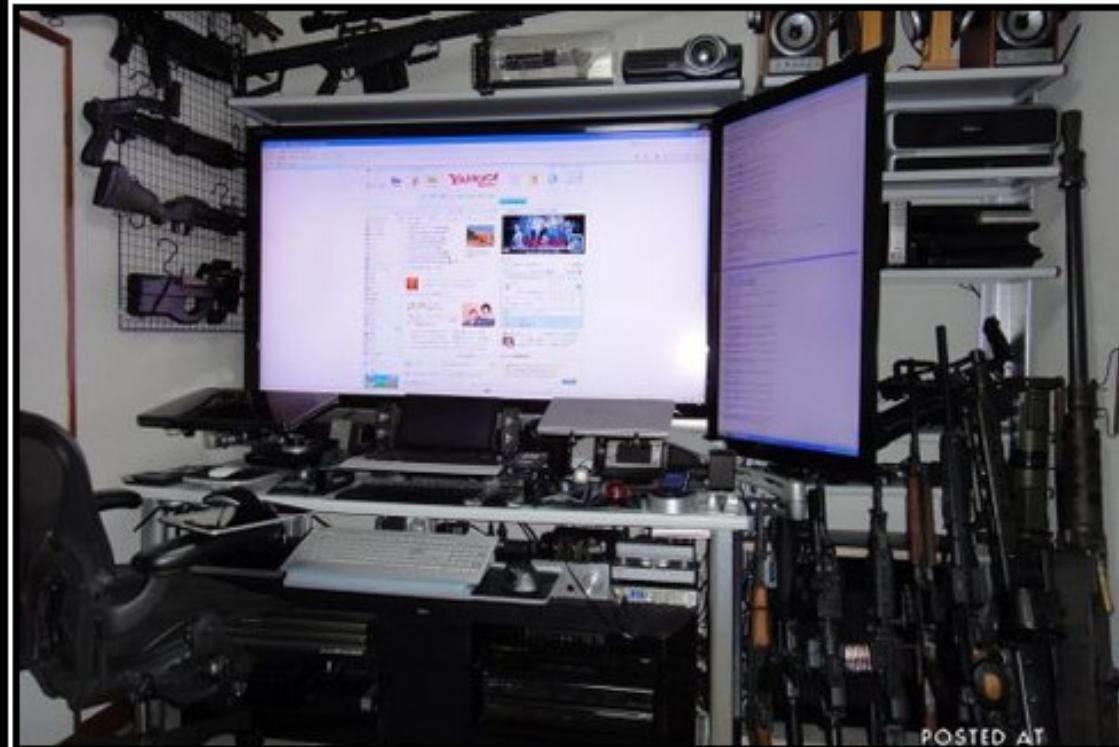
Countermeasures of theft

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



POSTED AT

WORKPLACE VIOLENCE

He may be a geek but you never know when he'll take his FPS to IRL!

fakeposters.com



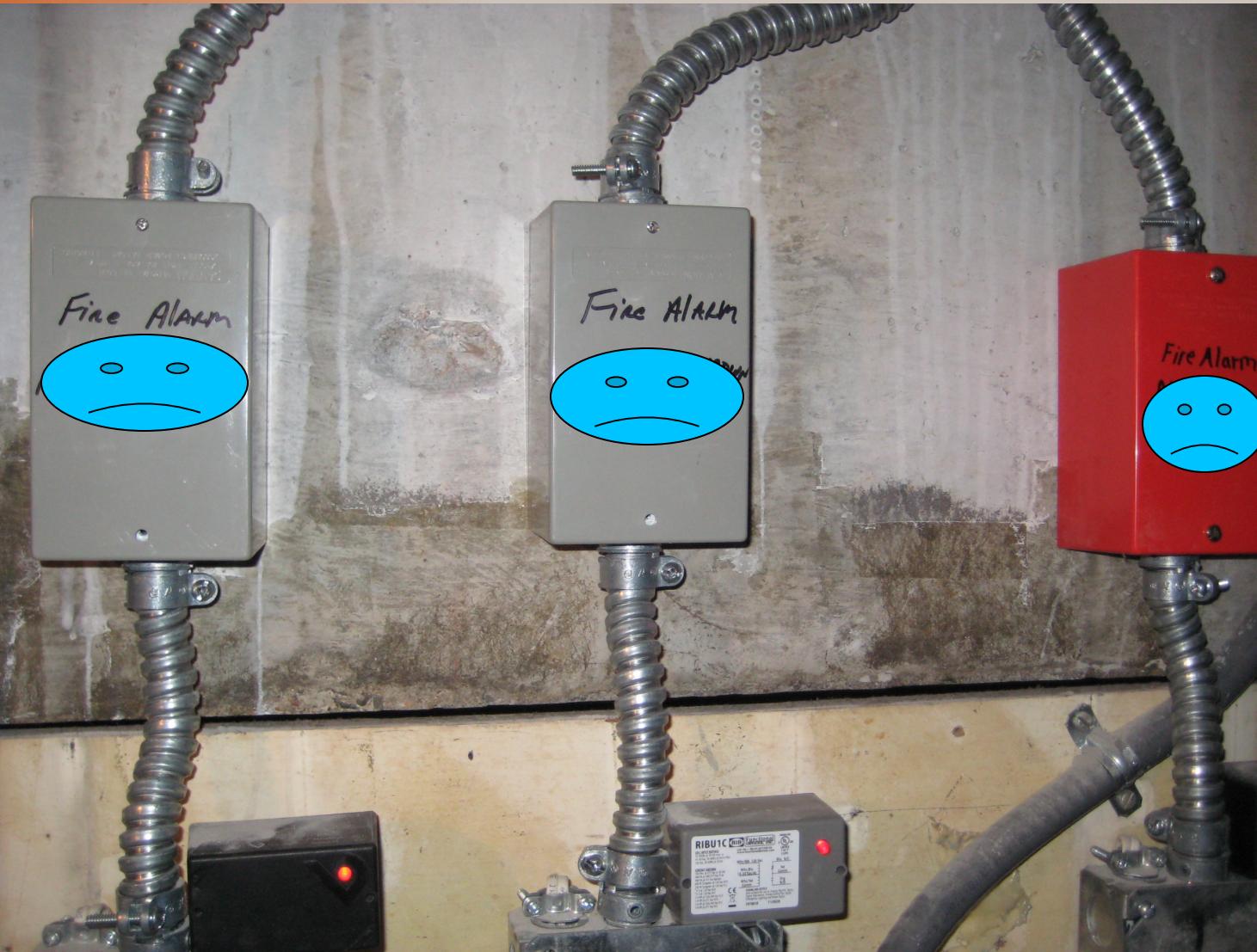
2. Kill Everyone



2. Kill Everyone



2. Kill Everyone



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
走为上



2. Kill Everyone



And just to bring it home...



2. Kill Everyone



2010.11.06 01:10:52

树上开花 反客为主 美人计
反间计 苦肉计 连环计

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
走为上计



STRATEGEM 1 SOLUTIONS
"DEFENSE THROUGH DISCOVERY"



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



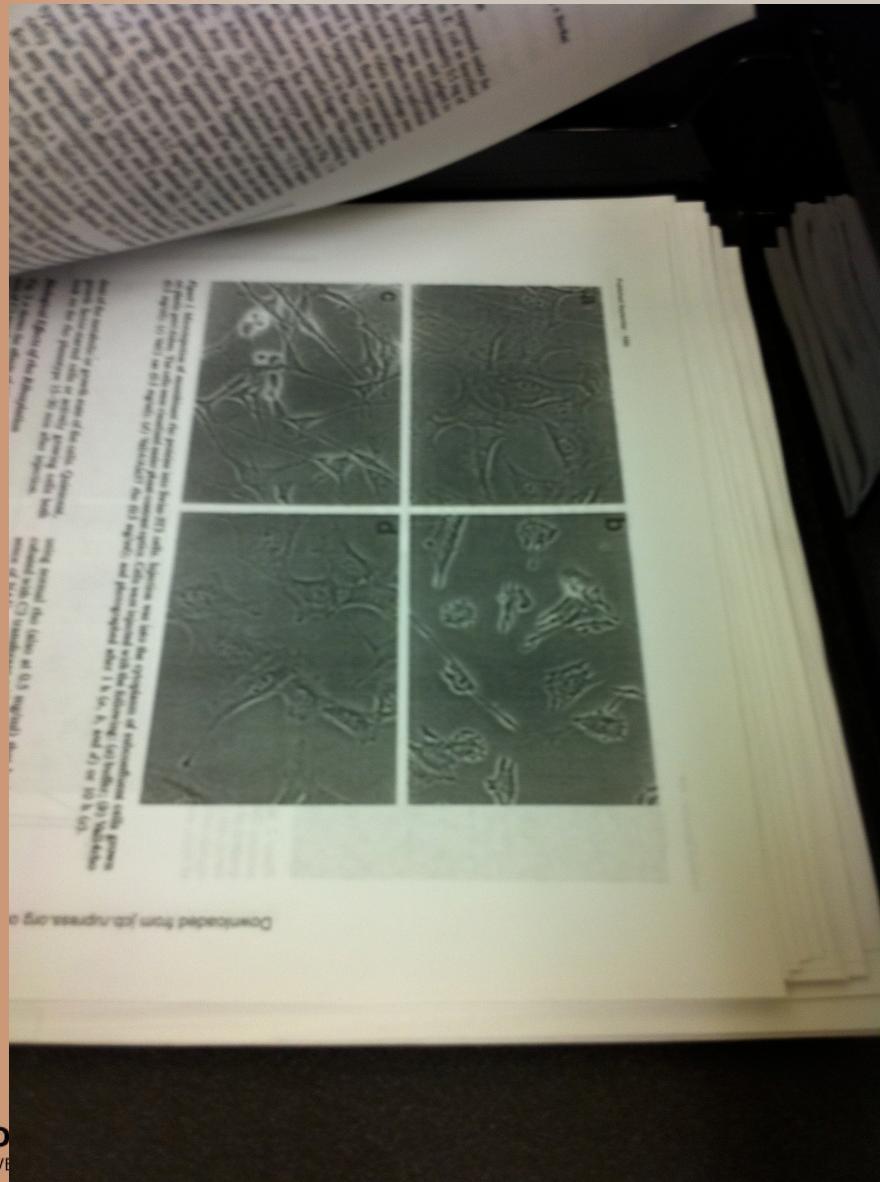
ESPIONAGE

There is a spy among us

逸待劳
渡陈仓
手牵羊
擒故纵
水摸鱼
道伐虢
屋抽梯
城计
为



3. Cause total Financial ruin

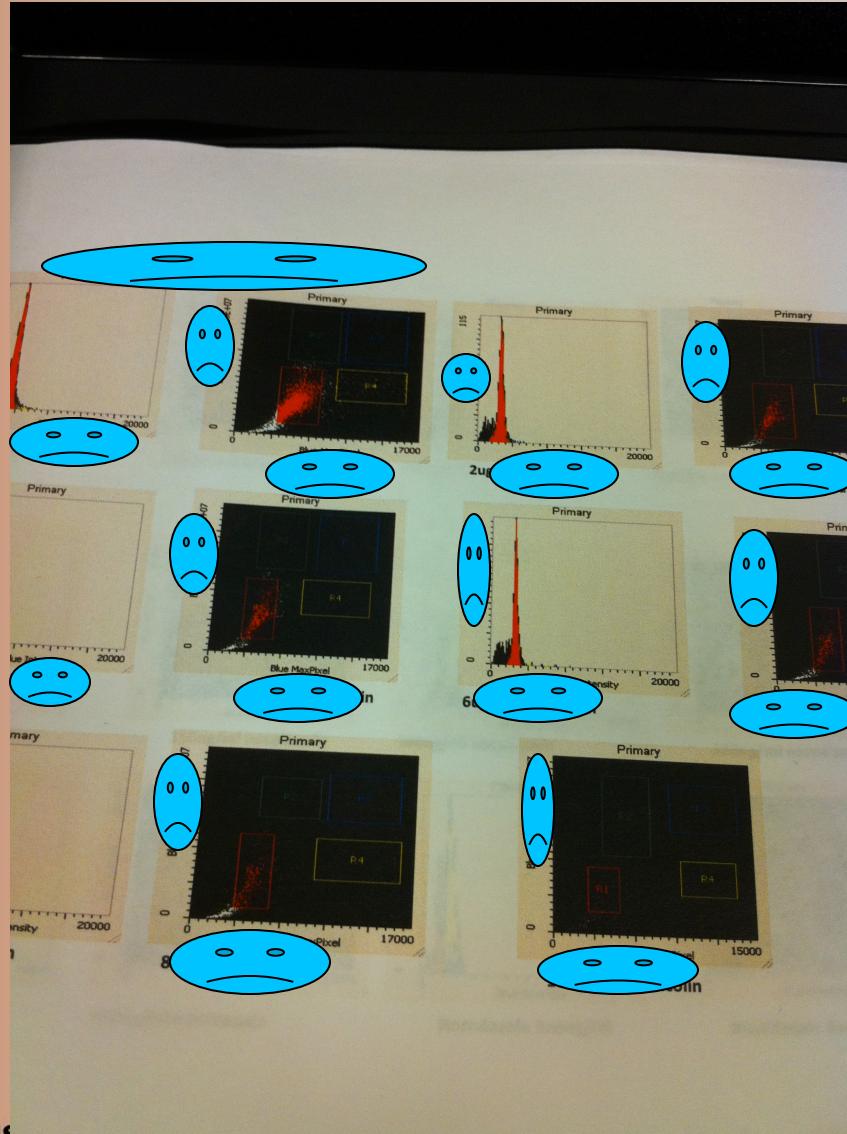


杀
生有
桃僵
离山
抽薪
近攻
不癲
计
计

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
走为上



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
走为上



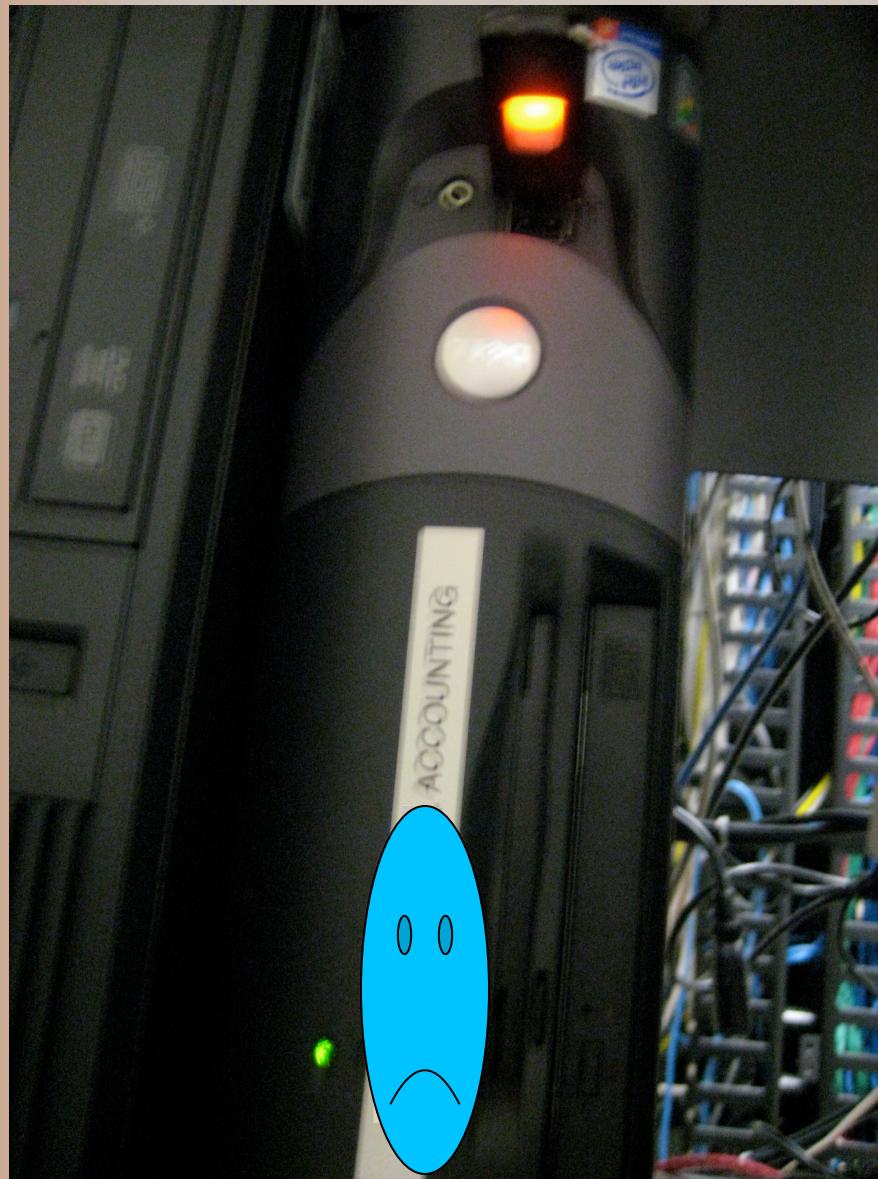
3. Cause total Financial ruin



3. Cause total Financial ruin



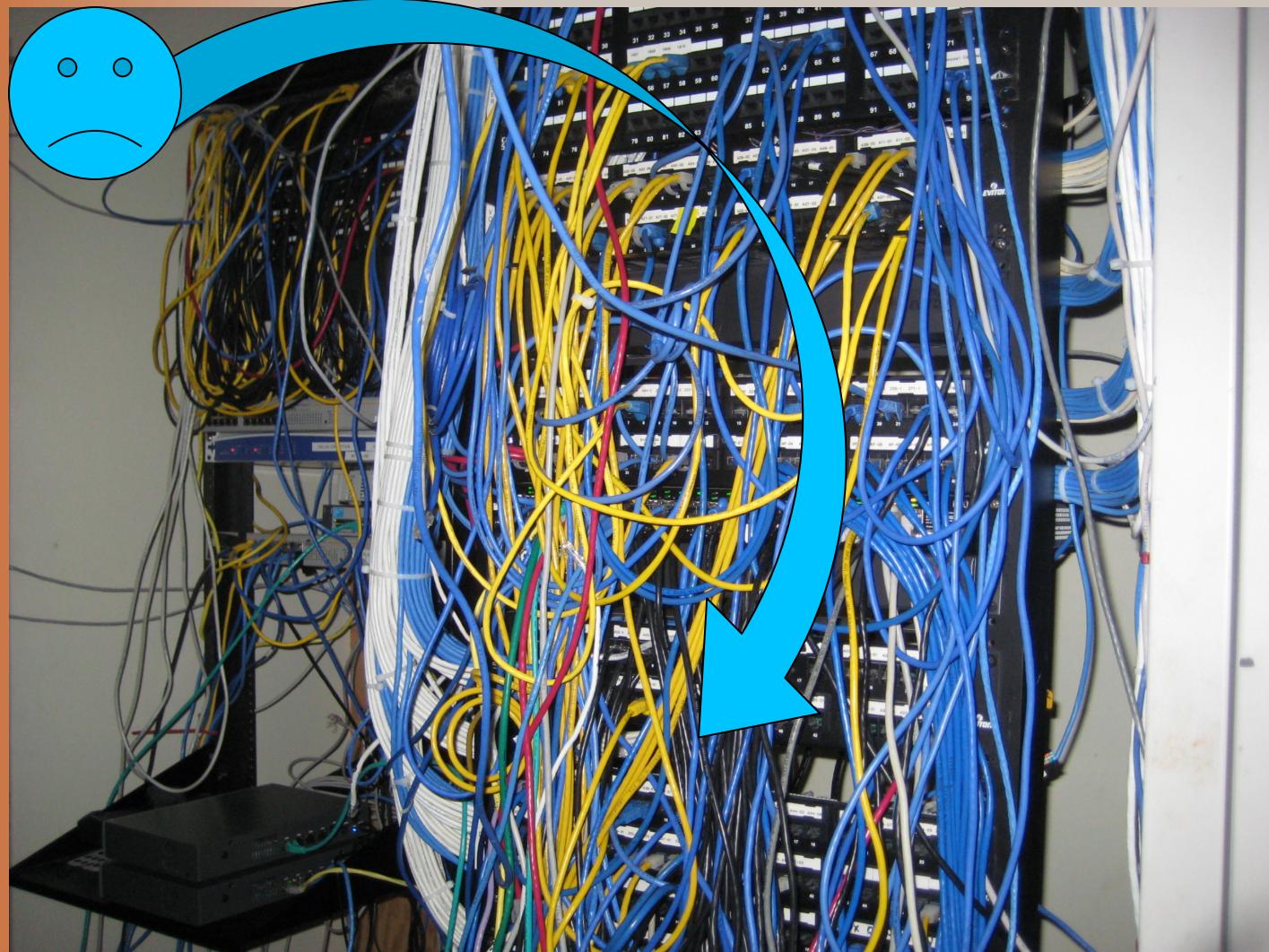
3. Cause total Financial ruin



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
走为上



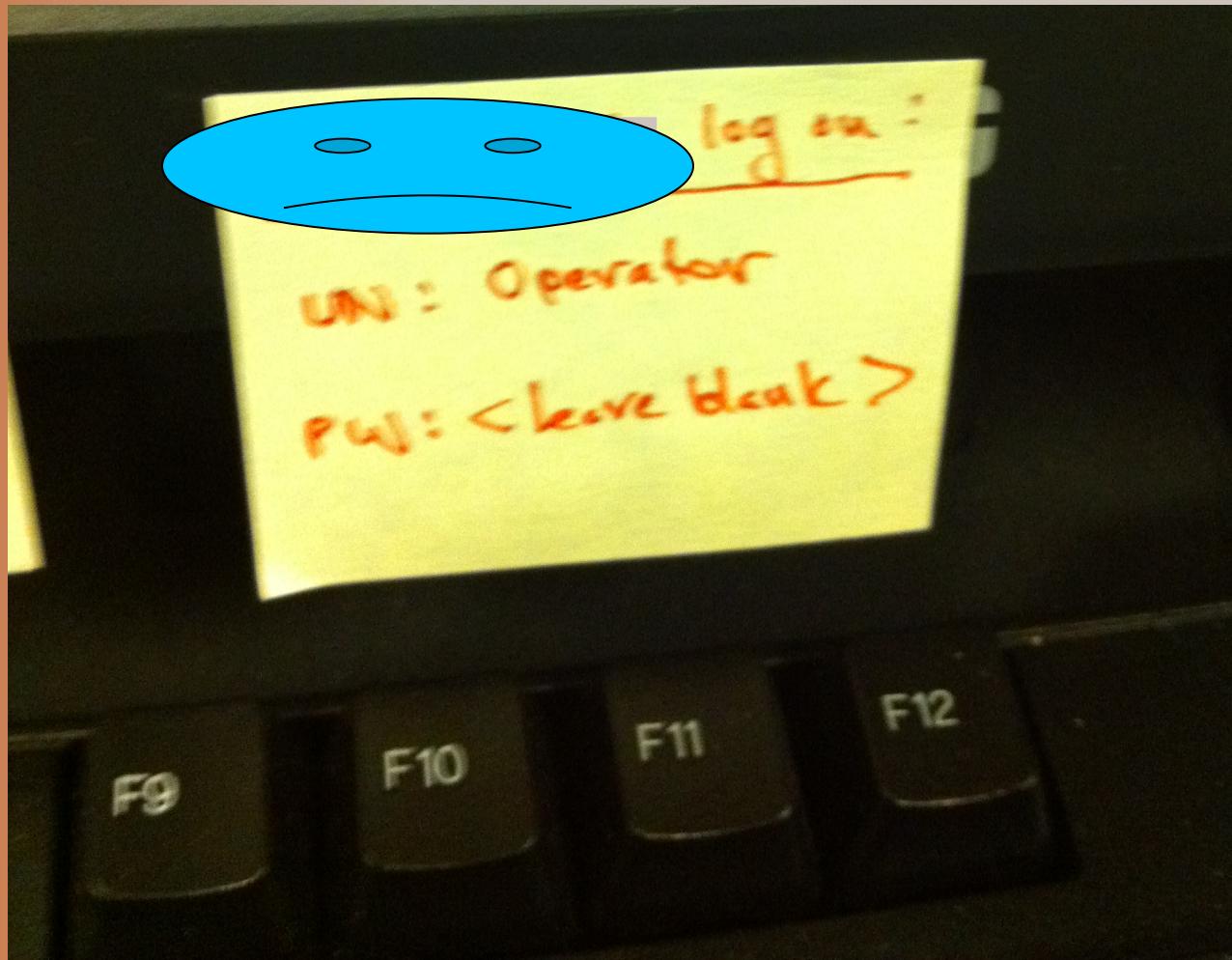
3. Cause total Financial ruin



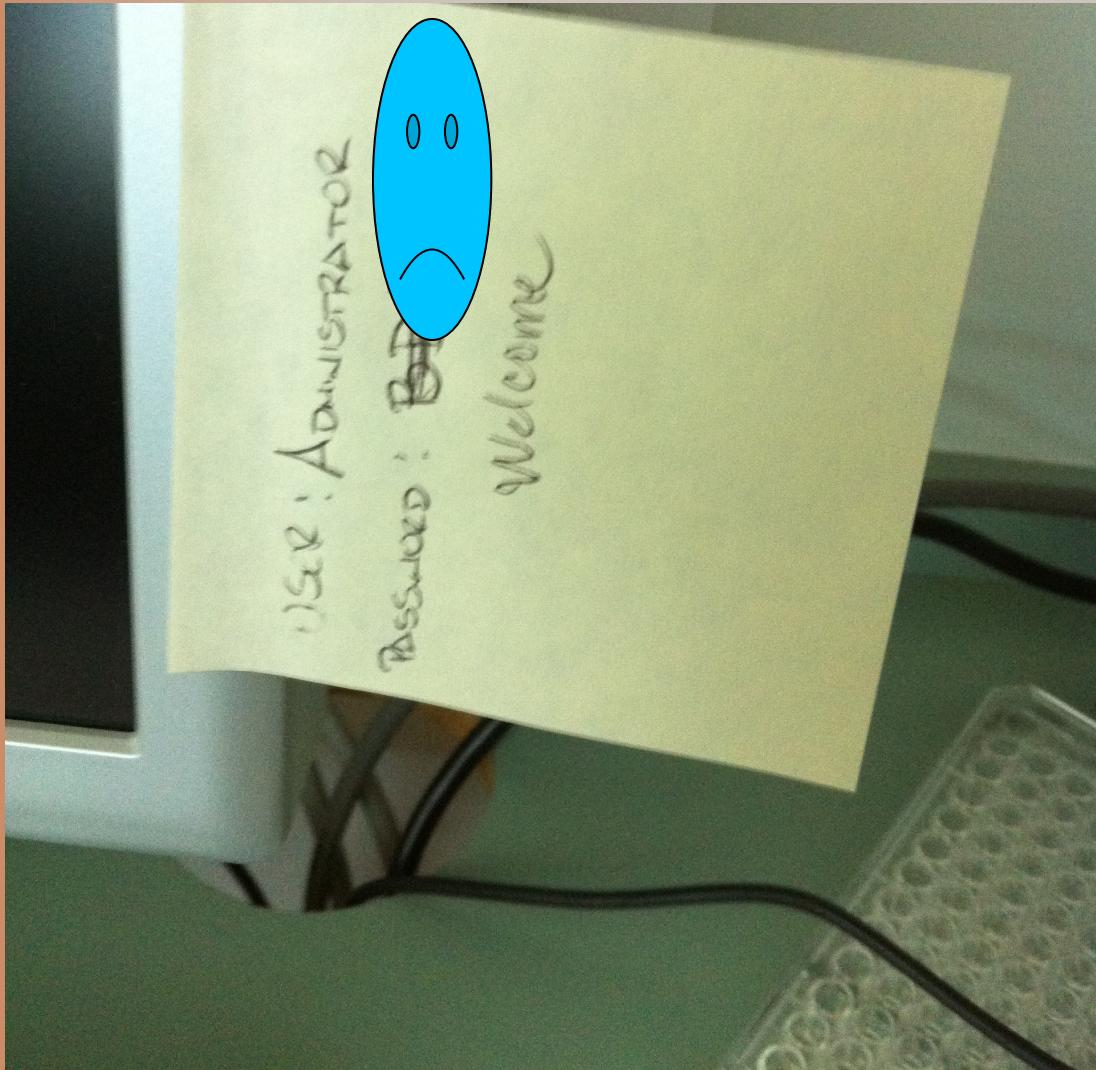
待劳
陈仓
牵羊
故纵
摸鱼
伐虢
抽梯
计



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
走为上



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
走为上



3. Cause total Financial ruin



3. Cause total Financial ruin



3. Cause total Financial ruin

Account | Wishlists | Fortunes | Bug Us
1-888-GEEKSTUFF or Live Chat

Welcome, Jayson!
(thinkgeek@0rb1dd3n.com) | logout

Loot: Your cart is lonely

SHOP BY CATEGORY SHOP FOR GIFTS WHAT'S NEW OMGWTFUN! GEEK POINTS CUSTOMER SERVICE

Home > Gadgets > Security & Spy Stuff >

Spy Keylogger



For recordkeeping, family security, or old fashioned snooping

- Records what people type for later review
- Spy on your kids, coworkers, parents
- Works with most wired keyboards
- [Read more...](#)

\$59.99 – \$74.99 (save up to 47%) **On Sale**

\$39.99 ✓ In stock

Please select...

Quantity:

BUY NOW or [add to wishlist](#)

Click to zoom

Main Description Additional Images

Earn Geek Points!

Yes, I want to accrue points to get free stuff when I buy other stuff! [\(Terms and Conditions\)](#)

[Sign me up!](#)

For recordkeeping, family security, or old fashioned snooping

Until such time as the CerebroSilica Brain-O-Matic 3000 interface between your grey-matter and your computer is invented, the best way to dump what's in your mind into your computer is through a keyboard. Everything from your quarterly sales figures to your personal private journal entry to your credit card numbers get typed into your keyboard.

Normally, you wouldn't worry about such things. You're careful with your passwords, keep your anti-virus up to date, and patch regularly so you're pretty sure your operating system is secure. Still, those keystrokes are recordable - all anyone needs is a tiny device the size of a fingertip, and suddenly all your deepest darkest secrets become public.

Naturally, we have that device. These keyloggers act as the "man-in-the-middle," monitoring each keystroke as it flies down your cable into your computer. You notice nothing, since every key you type gets dutifully

Sneaky



Spycam Car Key Fob Camera



Hollow Spy Coins



Phantom Keystroker V2



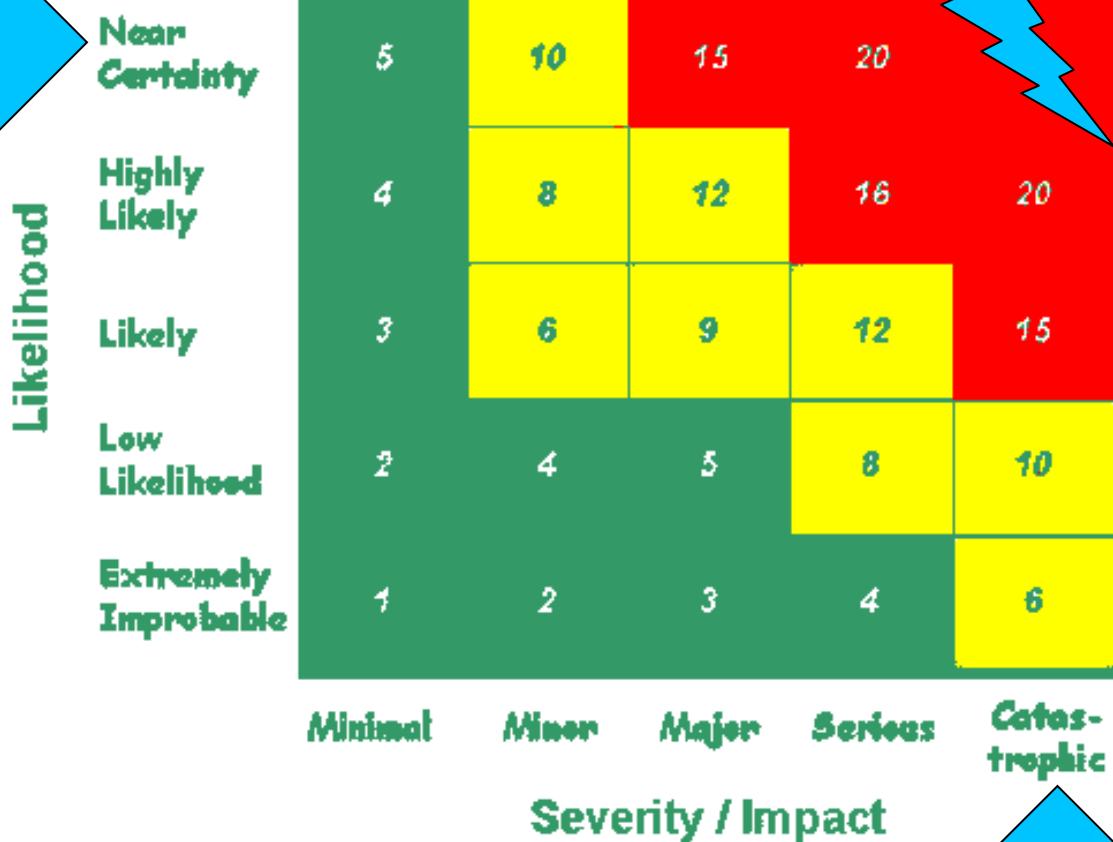
TV-B-Gone



STRATEGEM 1 S
"DEFENSE THROUGH DISCOVERY"

3. Cause total Financial ruin

Available at geek/gadget website



Risk Value Legend
 Low: ≤ 5 – Green
 Med: $> 5, \leq 12$ – Yellow
 High: > 12 – Red

Being able to log the CEO's Key Strokes



3. Cause total Financial ruin



反间计



苦肉计

连环计



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/>

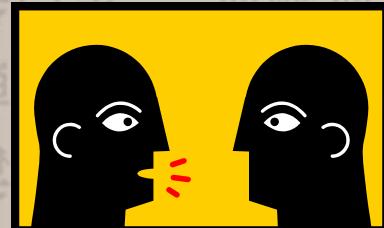
@jayonstreet on Twitter



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](#)

瞒天过海	围魏救赵	借刀杀人	以逸待劳
声东击西	无中生有	暗渡陈仓	
笑里藏刀	李代桃僵	顺手牵羊	
打草惊蛇	调虎离山	欲擒故纵	
金蝉脱壳	釜底抽薪	浑水摸鱼	
关门捉贼	远交近攻	假道伐虢	
指桑骂槐	假痴不癫	上屋抽梯	
树上开花	美人计	空城计	
反间计	连环计	走为上计	

