The Road to Hiring is Paved in Good Intentions

TRACE3

Timothy O’Brien

Director, Security Operations

- *NextGen SOC Concepts*
- *Security Operations Evolution*
- *Incident Response*
- *Threat Intelligence*
- *Digital Forensics*

Transformative IT Authority

As a 17-year information security professional, Mr. O’Brien is a subject matter expert in Computer Network Defense (CND)/blue team efforts, risk and incident management, intrusion and data analysis, and secure architecture design. Mr. O’Brien is well versed in developing technical solutions, determining the best options for the business and its goals, and creating comprehensive implementation plans that manages and minimizes risk for the organization. His excellent analytical and problem solving skills, with emphasis on understanding relationships among technical problems, result in sound and effective business solutions while reducing risk. He enjoys mentoring others and helping them develop their skills through supervisory positions, coursework development, mentoring, presenting at and helping run information security conferences, as well as instructional positions.

Disclaimer

This presentation is intended for the attendees and may contain information that is privileged or unsuitable for overly sensitive persons with low self-esteem, no sense of humour, or irrational religious/political beliefs. Those of you with an overwhelming fear of the unknown will be gratified to learn that there is no intended hidden message revealed by reading this warning backwards, so just ignore that alert notice from Microsoft. However, by pouring a complete circle of salt around yourself and your computer, you can ensure that no harm will befall you or your pets. Your mileage & satisfaction may vary, not all warranties apply during all time frames. Confirm these statements with your management before approval & implementation.

No individuals or equipment were harmed while producing this presentation, but it was created with recycled electrons. No animals were harmed in the transmission of this document, although if the raccoons keep getting into the trash I may have to do something about it. No individual, organization, or entity can be held liable or be quoted without written consent of the presenters.

I speak for no one, no one speaks for me.

Who Am I?

Who & What are you?

- Human
- Potentially a hiring manager
  - On the quest to hire information security professionals
  - People who will stay and grow with the company

Why are we talking about this?

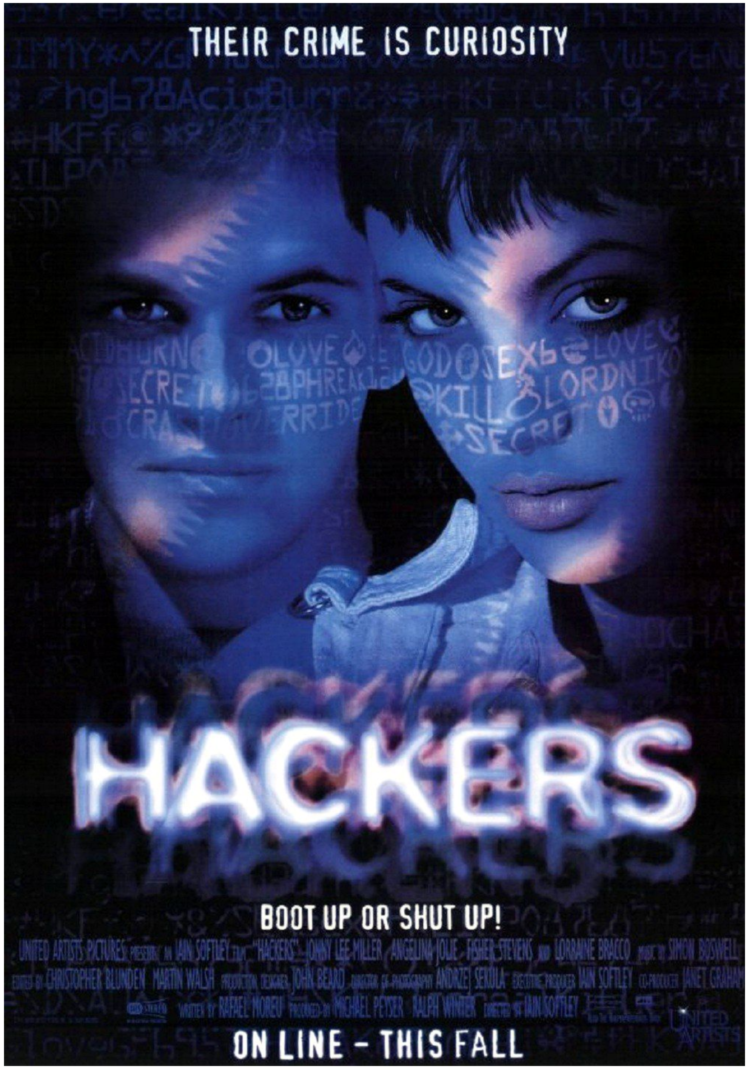
- Lots of talks about how to be a better pen tester and how to use all of the cool new tools, but only a few talks that address what some of us consider to be the hardest part of getting a job in InfoSec: the hiring process.
- We desperately need people with the technical skills hackers have
- Both sides of the table are doing horribly when it comes to hiring and interviewing for roles in the industry.

Why are we talking about this?

This talk takes my experiences (and that of others in the community) as both interviewers and interviewees in order to help better prepare hackers to enter (or move within) “the industry”.

We also want to let the people making hiring decisions know what they can do to get the people and experience they need.

Hackers??!!


THEIR CRIME IS CURIOSITY
HACKERS
BOOT UP OR SHUT UP!
UNITED ARTISTS PICTURES PRESENTS AN IAIN SOFTLEY FILM "HACKERS" JONNY LEE MILLER ANGELINA JOLIE FISHER STEVENS AND LORRAINE BRACCO MUSIC BY SIMON BOSWELL
EDITED BY CHRISTOPHER BLUNDEN MARTIN WALSH PRODUCTION DESIGNER JOHN BEARD DIRECTOR OF PHOTOGRAPHY ANDRZEJ SEKULA EXECUTIVE PRODUCER IAIN SOFTLEY CO-PRODUCER JANET GRAHAM
WRITTEN BY RAFAEL MOREU PRODUCED BY MICHAEL PEYSER RALPH WINTER DIRECTED BY IAIN SOFTLEY
UNITED ARTISTS
ON LINE - THIS FALL

MIT TMRC and TX-0

Why are we talking about this?

- "It is hard to find people to hire"
- We scare and confuse HR/recruiters
  - We are weird shits, that like to do weird things
  - The "evil hackers!!!111" OH NOOOESSS!
- We (hackers and hiring managers alike) keep shooting ourselves in this process
- Getting and retaining talent is in some ways a social engineering exercise
  - An exercise of "managing up"

Social Engineering Exercise
(Hiring Manager's Perspective)

- Get individuals interested in applying
- Avoid bottlenecks at HR
- Finding an appropriate candidate that upper management approves of
- Getting an appropriate offer that upper management approves of
- The acceptance of the offer by the candidate
- Having the candidate show up on day one and onboarded
- Nurturing the candidate so they grow personally and professionally

Breakdown

- Setting expectations
  - By hiring manger, HR, leadership, etc.
- Application process
  - Resume gathering / submissions
- Interviews
- Closing the deal (post-interview)
- Perspective & expectations

Core Problem aka Opportunity #1

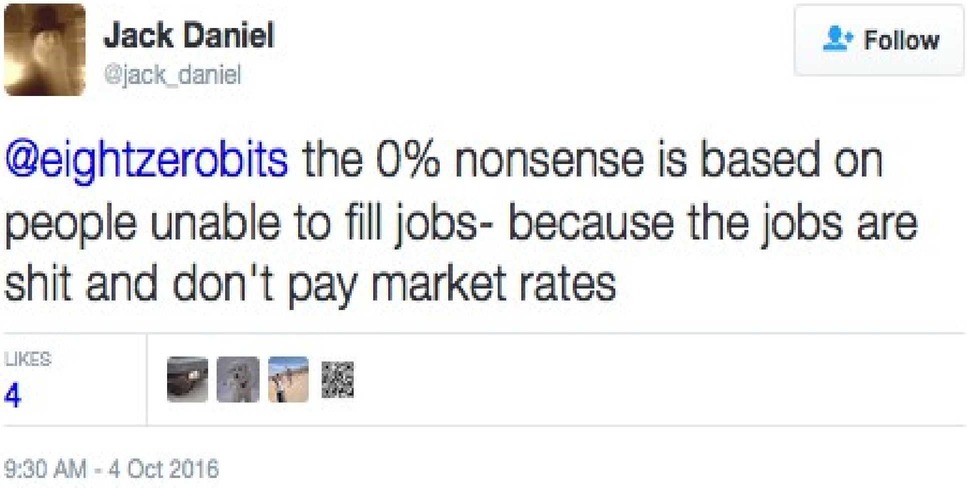
Expectations

Expectations

"Can't find anyone to hire!"

vs

"Must work in our corporate office in Wichita, initially on a six month contract to fire with a rotating SOC shift cycle. Oh, and you start on night shift."



Jack Daniel
@jack_daniel

@eightzerobits the 0% nonsense is based on people unable to fill jobs- because the jobs are shit and don't pay market rates

LIKES
4

9:30 AM - 4 Oct 2016

Readjust Expectations

“Over the years, what we have essentially done—intentionally or not—is create a sub-category of talent whom we will never hire. The Unhireable. …

-Winn Schwartau, “*Hiring the unhireable*”

Manager, What do you want?

- Expectations for jobs can be unclear
- The job title may say a “Junior” or “Entry-level”, but then it asks for CISSP certification or 5 years of experience
- Position Description (PD) could be all over the map, looking for jack of all trades (master of none)
- Folks looking to break into InfoSec end up either applying for everything or nothing
- They honestly have no idea what hiring managers are looking for, but they want to try regardless.

Tell us what you need

- What you really, really want?

  What do you need?

- Be clear with what the job will entail
- If you want a log monkey, say you want a log monkey.

Manager, What do you need?

- What really matters?

  To your environment, your team, the biz?
- Experience?

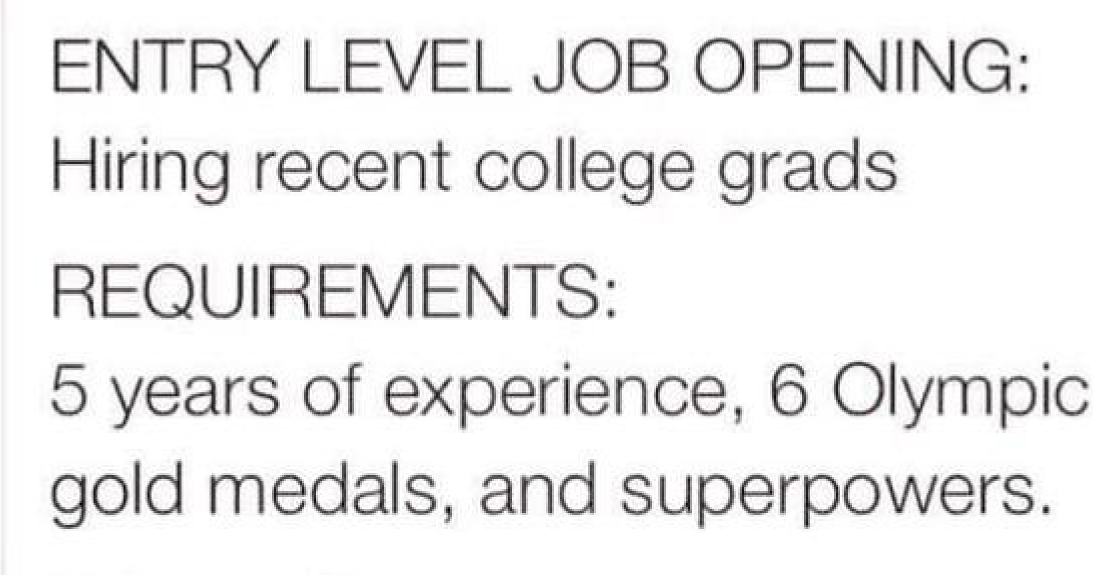
  Entry-level or someone more senior

  What level of experience can you afford?
- Certs and/or a degree?
- Do not ask for things “just because”

  Limits your pool of applicants

Manager, What do you need?

- Consider what really matters
  - Getting past HR
  - Experience
    - Need vs affordability
- Conciseness can reduce the likelihood of alienating potential applicants



ENTRY LEVEL JOB OPENING:

Hiring recent college grads

REQUIREMENTS:

5 years of experience, 6 Olympic gold medals, and superpowers.

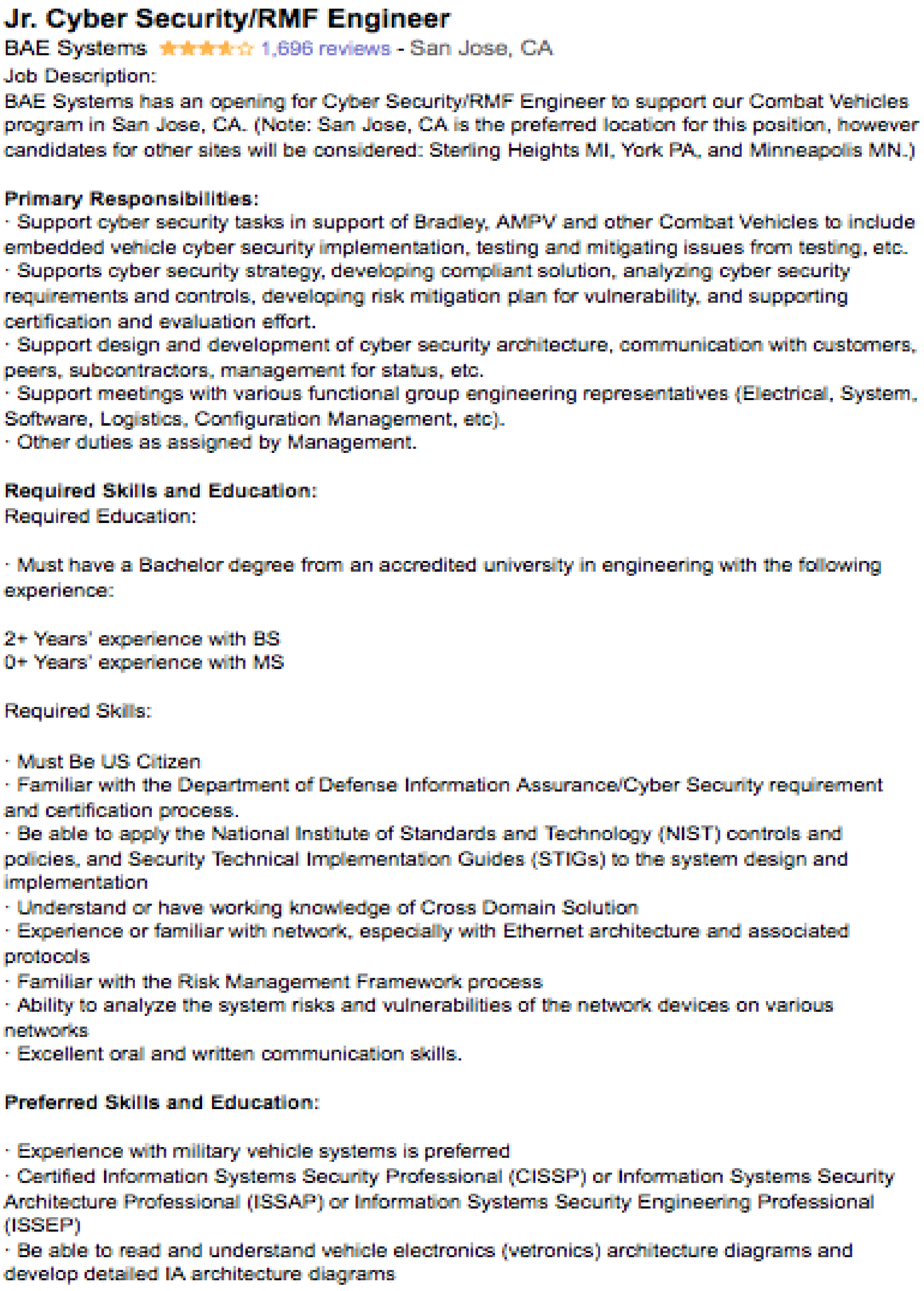
Certifications and degrees

- Are they directly relevant to the position?
- Can the business afford reimbursement if passed within a certain amount of time

CORPORATE DILEMMA
WHAT IF WE TRAIN THEM AND THEY LEAVE?
WHAT IF WE DON'T... AND THEY STAY?
INVESTING IN EMPLOYEES

Realistic?

- Are they possible?
  - Two years experience
  - CISSP, ISSAP, ISSEP preferred



Jr. Cyber Security/RMF Engineer

BAE Systems ★★★★☆ 1,696 reviews - San Jose, CA

Job Description:

BAE Systems has an opening for Cyber Security/RMF Engineer to support our Combat Vehicles program in San Jose, CA. (Note: San Jose, CA is the preferred location for this position, however candidates for other sites will be considered: Sterling Heights MI, York PA, and Minneapolis MN.)

Primary Responsibilities:

· Support cyber security tasks in support of Bradley, AMPV and other Combat Vehicles to include embedded vehicle cyber security implementation, testing and mitigating issues from testing, etc.
· Supports cyber security strategy, developing compliant solution, analyzing cyber security requirements and controls, developing risk mitigation plan for vulnerability, and supporting certification and evaluation effort.
· Support design and development of cyber security architecture, communication with customers, peers, subcontractors, management for status, etc.
· Support meetings with various functional group engineering representatives (Electrical, System, Software, Logistics, Configuration Management, etc).
· Other duties as assigned by Management.

Required Skills and Education:

Required Education:

· Must have a Bachelor degree from an accredited university in engineering with the following experience:

2+ Years' experience with BS
0+ Years' experience with MS

Required Skills:

· Must Be US Citizen
· Familiar with the Department of Defense Information Assurance/Cyber Security requirement and certification process.
· Be able to apply the National Institute of Standards and Technology (NIST) controls and policies, and Security Technical Implementation Guides (STIGs) to the system design and implementation
· Understand or have working knowledge of Cross Domain Solution
· Experience or familiar with network, especially with Ethernet architecture and associated protocols
· Familiar with the Risk Management Framework process
· Ability to analyze the system risks and vulnerabilities of the network devices on various networks
· Excellent oral and written communication skills.

Preferred Skills and Education:

· Experience with military vehicle systems is preferred
· Certified Information Systems Security Professional (CISSP) or Information Systems Security Architecture Professional (ISSAP) or Information Systems Security Engineering Professional (ISSEP)
· Be able to read and understand vehicle electronics (vetronics) architecture diagrams and develop detailed IA architecture diagrams

Scoping The Role

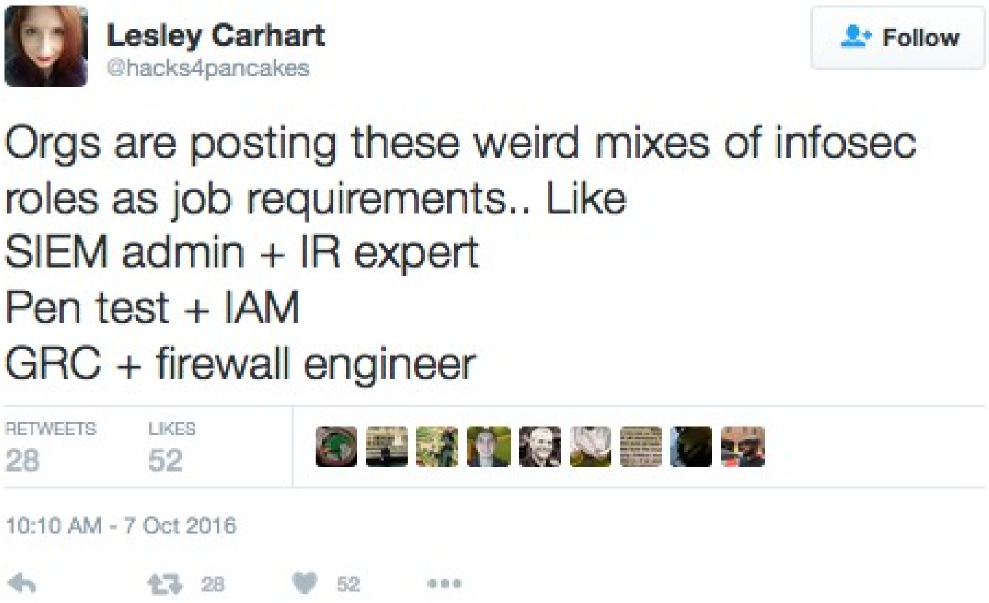
- Contractor or full time employee?
- Specialty roles versus “Jack of All Trades”
  - Both have their benefits and drawbacks
  - Consider type of specialty roles (analysts, engineers, architects)
- State the realm that applicants will be working in
  - Application, network, or system security?
  - Vendor-specific preferences

Scope

- Dedicated role
    - Analyst (Digging through the data)
    - Engineer (Running the toolsets)
    - Architect (Strategic view)
    - Forensics
    - Malware
    - Penetration tester
- Application vs Network/System Security
- Vendor, developer of software/hardware

ALL THE THINGS!!!111

- 'Jack of all trades'?
  - Master of none
  - Consider career growth
  - Health & welfare of team
  - Burnout



Lesley Carhart
@hacks4pancakes

Orgs are posting these weird mixes of infosec roles as job requirements.. Like
SIEM admin + IR expert
Pen test + IAM
GRC + firewall engineer

RETWEETS 28
LIKES 52

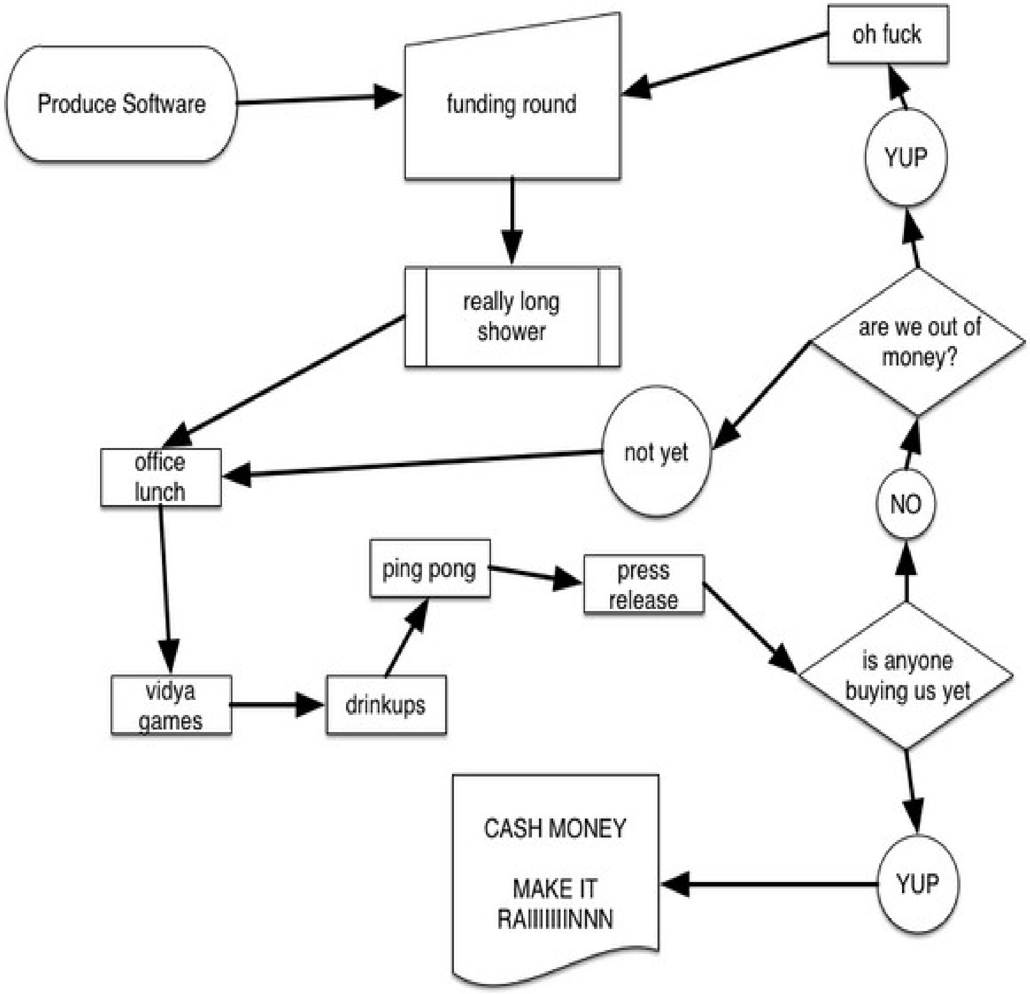
10:10 AM - 7 Oct 2016

Where do they fit?

- Organizational placement & fit
    - Who will be their direct report(s)?
    - Report to?
- Does the team report to IT, compliance, or Legal?
    - Consider conflicts of interest
- Over-extension of new and current employees
- Start ups & small companies

Fit Within A Startup

- A Security Architect is not a replacement for a CISO
  - Consultant recommended approach
- Question leadership & food chain



Contractor or FTE?

- What do those “temp to fire” roles say about your company and your leadership?
  - Cycling through folks till they find the “right fit”
    - AKA, never hire
    - All risk on the individual
- There is a difference between the hired gun (contractor/consultant) being brought in for a specific project/task/problem, and the abuse of individuals and the system

Contractor class

- Paid recruiters, overseas body shops are helping perpetuate the "contractor class"
  - "Temp to fire" roles
  - Only interviewing & hiring through the bodyshop
  - Ignoring those internal/external applicants
- Many hackers ignore these bodyshops, so what quality candidates are you getting?
- Creating another class of un-hireables, feeding this contractor ecosystem
- And the cycle goes on… feeding those bodyshops we hate and robbing us

Questioning Compensation

- Salary history

  You know the range, pay them what they are worth

- Incentives

  Flexible work schedule, PTO

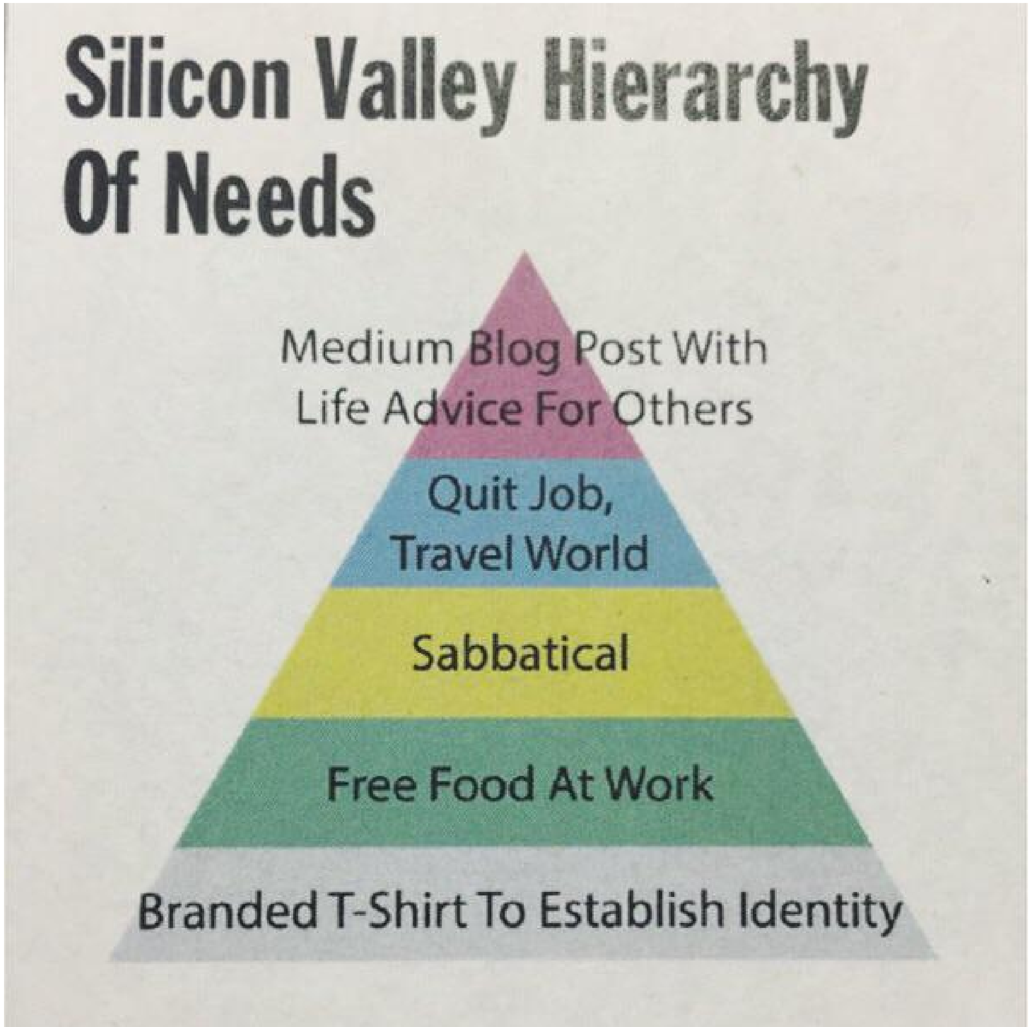
  Work from home/remote

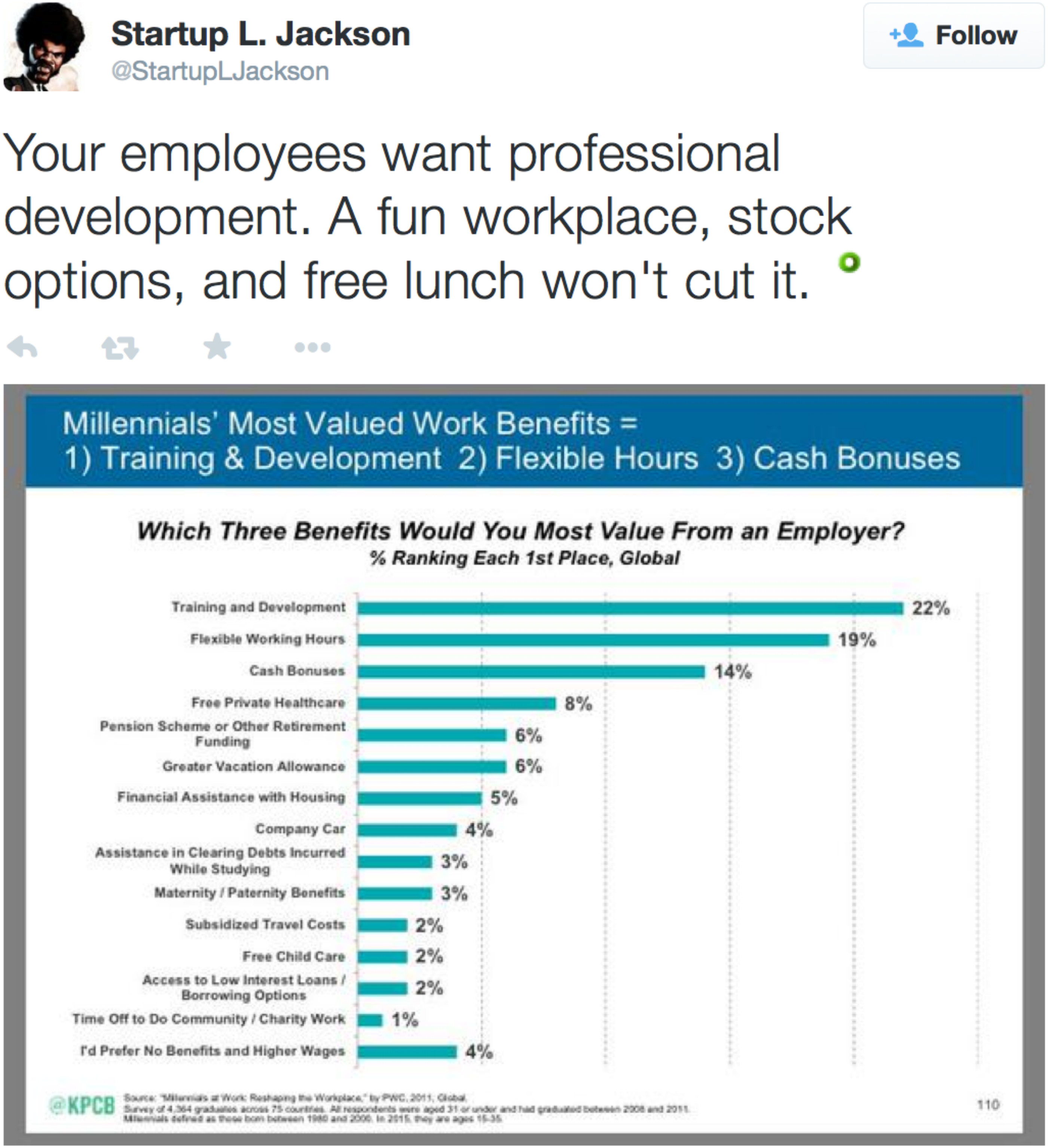
  Training budget

  Conferences

  Lab gear

  Title & career/personal growth


Silicon Valley Hierarchy Of Needs
Medium Blog Post With Life Advice For Others
Quit Job, Travel World
Sabbatical
Free Food At Work
Branded T-Shirt To Establish Identity



Startup L. Jackson
@StartupLJackson

Your employees want professional development. A fun workplace, stock options, and free lunch won't cut it.

Millennials' Most Valued Work Benefits =
1) Training & Development 2) Flexible Hours 3) Cash Bonuses

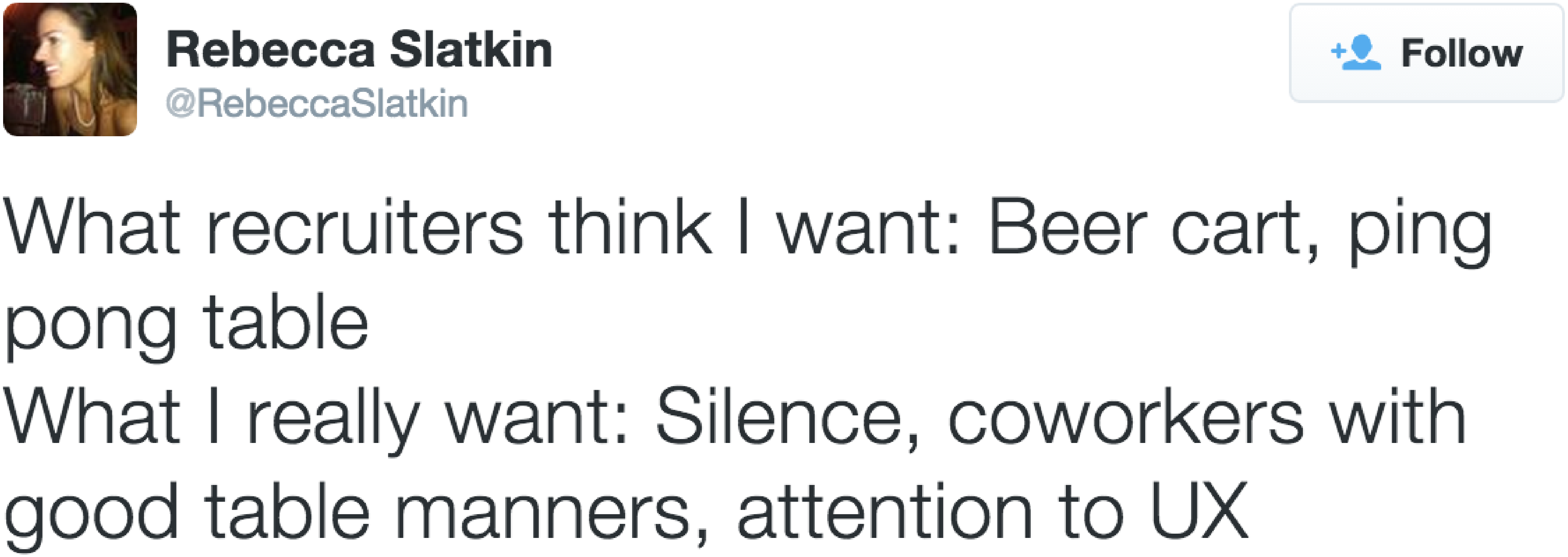
Which Three Benefits Would You Most Value From an Employer?
% Ranking Each 1st Place, Global

Training and Development 22%
Flexible Working Hours 19%
Cash Bonuses 14%
Free Private Healthcare 8%
Pension Scheme or Other Retirement Funding 6%
Greater Vacation Allowance 6%
Financial Assistance with Housing 5%
Company Car 4%
Assistance in Clearing Debts Incurred While Studying 3%
Maternity / Paternity Benefits 3%
Subsidized Travel Costs 2%
Free Child Care 2%
Access to Low Interest Loans / Borrowing Options 2%
Time Off to Do Community / Charity Work 1%
I'd Prefer No Benefits and Higher Wages 4%

@KPCB

Source: "Millennials at Work: Reshaping the Workplace," by PWC, 2011, Global.
Survey of 4,364 graduates across 75 countries. All respondents were aged 31 or under and had graduated between 2008 and 2011.
Millennials defined as those born between 1980 and 2000. In 2015, they are ages 15-35.

110



Rebecca Slatkin
@RebeccaSlatkin

What recruiters think I want: Beer cart, ping pong table
What I really want: Silence, coworkers with good table manners, attention to UX

Core Problem aka Opportunity #2
The Application Process

ALREADY UPLOADED YOUR RESUME?
BETTER MAKE YOU RETYPE OUT YOUR ENTIRE WORK HISTORY AND EXPERIENCE

The Application Process

- Preparation is key, and before the first calls are made to set up an interview
  - Seldom done, let alone done well
- Timing is everything
  - Candidate could have finished the application process, hired, and started elsewhere before you send your first reply

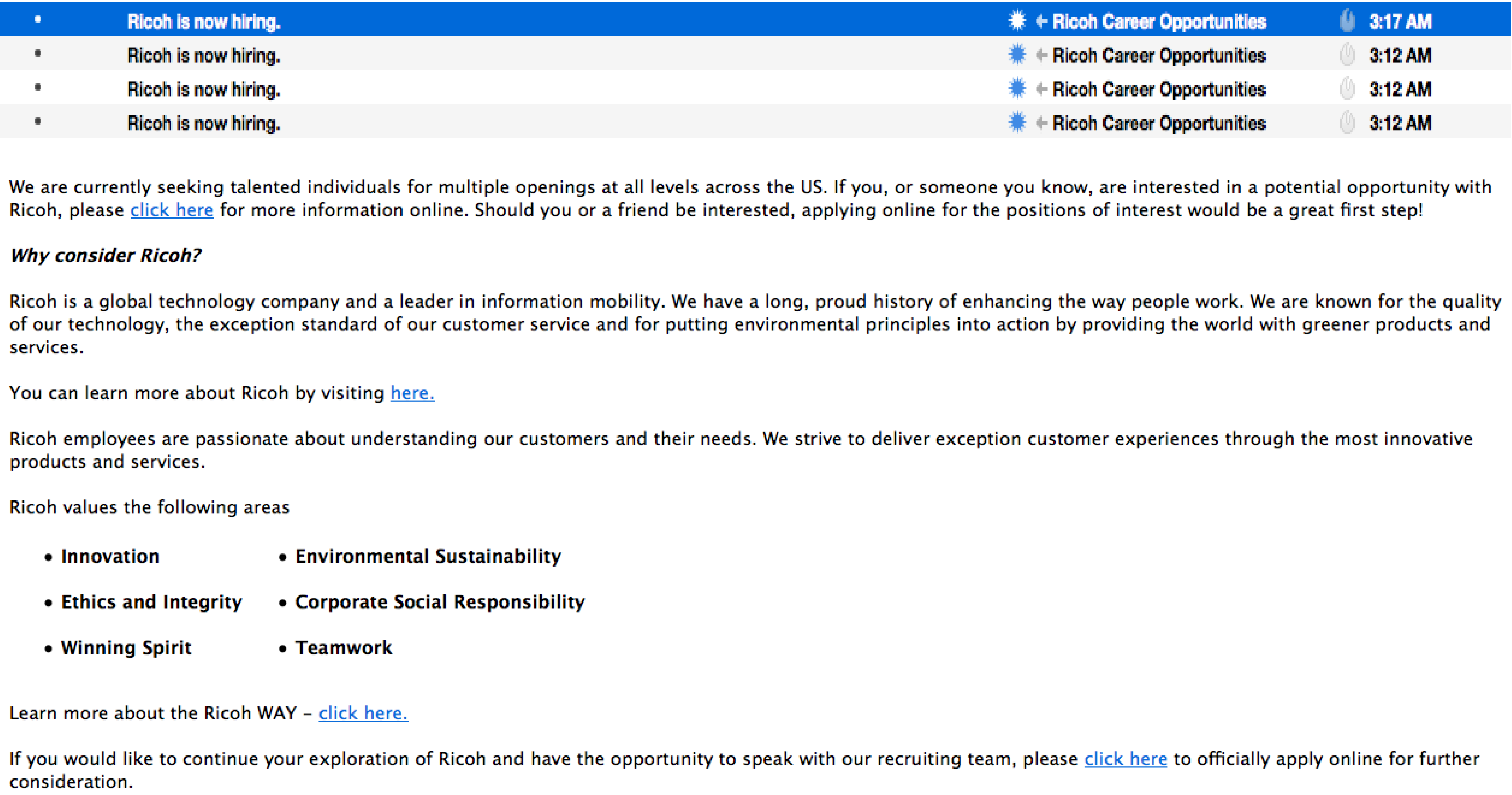
How Do You Find Candidates?

- In person, get out of our bubble, out of our echo chamber
- Attend, or even get involved in your
  - Local IT & InfoSec communities, LUG/user groups
  - Meetup.com groups
  - Mailing lists and forums, Slack & IRC channels (#2600)
  - Local tech/colleges
  - Professional association meetings
  - Hacker & Maker spaces, hamfests/Electronic Flea Market (EFM)
- Join the folks at Reddit CitySec gatherings (SiliSec, BaySec, & HoodSec) and 2600

How Do You Find Candidates?

- Posting online
  - Monster, CareerBuilder, Beyond, Indeed, etc.
  - Craigslist
  - Technical & topic related forums on Reddit, Stack Overflow, etc.
- Work with your marketing team for social media exposure
- Closed, invite only IT/InfoSec communities & lists
- Boutique recruiters (NinjaJobs.org)
- Meetup.com forums, local LUG, LISA, tech communities

Bad Outreach



•	Ricoh is now hiring.	✹ ← Ricoh Career Opportunities	3:17 AM
•	Ricoh is now hiring.	✹ ← Ricoh Career Opportunities	3:12 AM
•	Ricoh is now hiring.	✹ ← Ricoh Career Opportunities	3:12 AM
•	Ricoh is now hiring.	✹ ← Ricoh Career Opportunities	3:12 AM

We are currently seeking talented individuals for multiple openings at all levels across the US. If you, or someone you know, are interested in a potential opportunity with Ricoh, please click here for more information online. Should you or a friend be interested, applying online for the positions of interest would be a great first step!

Why consider Ricoh?

Ricoh is a global technology company and a leader in information mobility. We have a long, proud history of enhancing the way people work. We are known for the quality of our technology, the exception standard of our customer service and for putting environmental principles into action by providing the world with greener products and services.

You can learn more about Ricoh by visiting here.

Ricoh employees are passionate about understanding our customers and their needs. We strive to deliver exception customer experiences through the most innovative products and services.

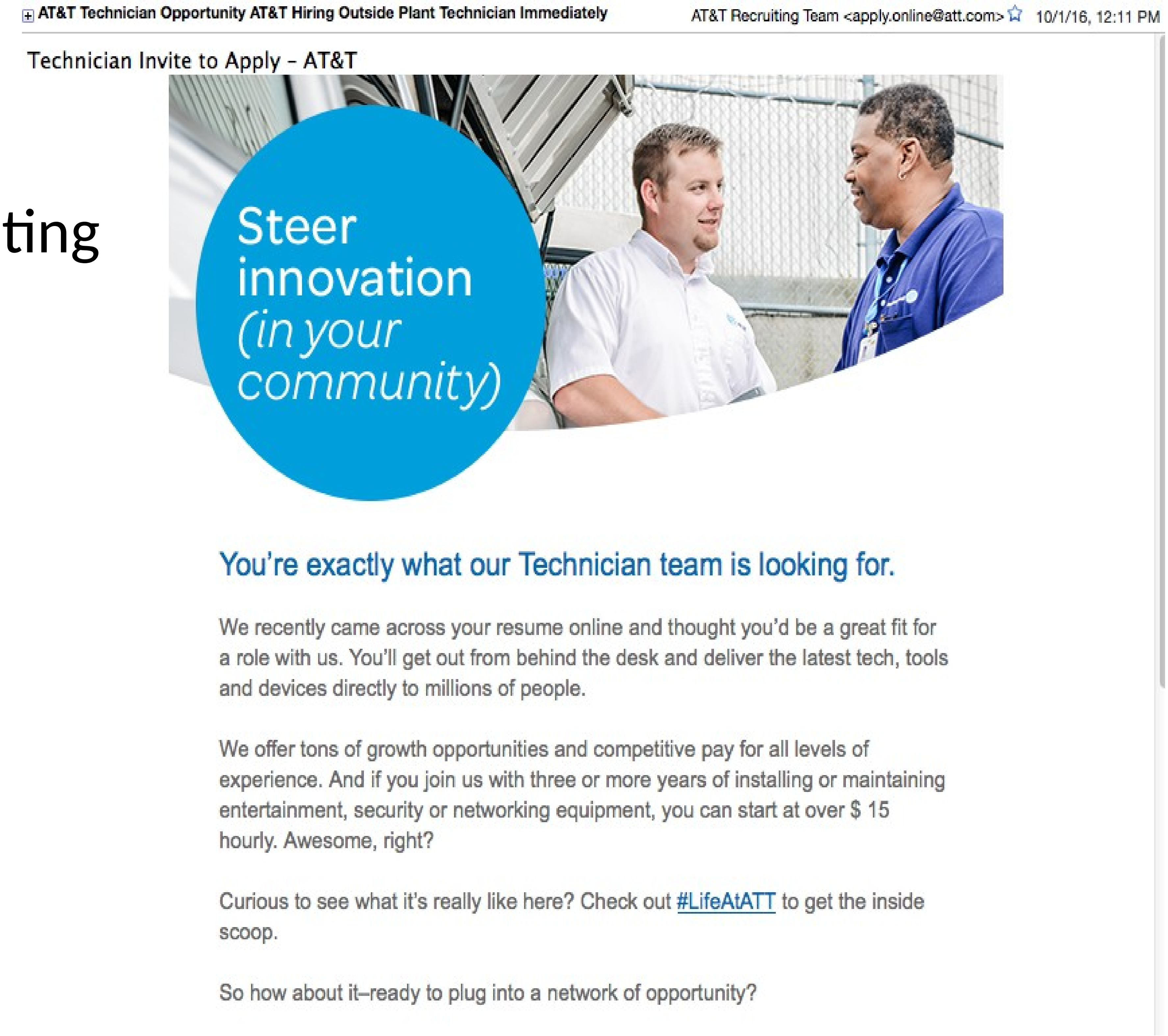
Ricoh values the following areas

- **Innovation**
- **Ethics and Integrity**
- **Winning Spirit**
- **Environmental Sustainability**
- **Corporate Social Responsibility**
- **Teamwork**

Learn more about the Ricoh WAY – click here.

If you would like to continue your exploration of Ricoh and have the opportunity to speak with our recruiting team, please click here to officially apply online for further consideration.

Bad Targeting



AT&T Technician Opportunity AT&T Hiring Outside Plant Technician Immediately   AT&T Recruiting Team <apply.online@att.com>   10/1/16, 12:11 PM

Technician Invite to Apply - AT&T

You're exactly what our Technician team is looking for.

We recently came across your resume online and thought you'd be a great fit for a role with us. You'll get out from behind the desk and deliver the latest tech, tools and devices directly to millions of people.

We offer tons of growth opportunities and competitive pay for all levels of experience. And if you join us with three or more years of installing or maintaining entertainment, security or networking equipment, you can start at over $ 15 hourly. Awesome, right?

Curious to see what it's really like here? Check out #LifeAtATT to get the inside scoop.

So how about it–ready to plug into a network of opportunity?

What Is Your Role In Talent?

- One of your obligations as a hiring manager, as a leader in InfoSec is to nurture talent in our field
- Your involvement in the local groups helps promote (your team, your company, the industry) & screen potential candidates
- If you want talent, YOU have to work it, stop decrying the talent shortage as out of your hands, we have a responsibility to grow talent as much as utilize talent.
- More than a lack of talented technical staff, or a lack of will at upper management, is a gap in middle management. Middle management does staffing, actually goes out and spends budget, and ensures best practices for everything. When there is a failure here, the whole thing falls apart.

RECRUITER ADDED ME ON LINKEDIN
SO I GUESS YOU COULD SAY THINGS ARE GETTING PRETTY SERIOUS
makeameme.org

Recruiters

- There are different types of technical recruiters
    - Company
    - Agencies (boutique and otherwise)
- Agencies just looking for a body to fill a seat
    - Overseas body shops
    - Spamming of the PDs, unable to answer follow-up questions
    - Helping perpetuate the sub class of contractor/consultant workers
    - Are they really finding unique talent, or just the same folks that already applied to your role?

HR/recruiter teams

- Is your Recruiter roadblocks or helping you attract talent?
  - Your HR/recruiting staff and their initial contacts and conversations with candidates set the tone for the process, ensure they are good ones. Should be setting up expectations for the process.
  - Are they helping source, or just screening? Neither?
- Demands for current and past salary history
- Sends the screening questionnaire, expecting the applicant to do their work
  - Starts off with a poor experience
  - Candidates will go elsewhere, after asking what is the ROI?
- Your HR/recruiting staff and their initial contacts and conversations with candidates set the tone for the process, ensure they are good ones
  - Sets up expectations for the next step(s)
  - Have someone from HR on your Incident Response (IR) team
  - Does your recruiter join you in interviews? Why not?

External Recruiters

- Do your research on recruiters like you would potential companies to work for
  - Build relationships with good ones
  - NinjaJobs.com
- Look out for frauds and scams
- Lookup: Why 'True Recruiters' are actually Super Unicorns

Managing The Applications

- There are different Application Tracking Systems (ATS)
  - Heavyweight application systems with data mining looking for keywords & application management
    - Taleo, iCIMS, SuccessFactors, PeopleSoft, Bullhorn, Brassring
  - Lightweight application tracking
    - Workday, Jobvite, SilkRoad, LinkedIn, Greenhouse, SmartRecruiter
  - Human
    - Email and spreadsheet
- Each have pro/cons, from an applicant & manager perspective
  - What is the ROI?

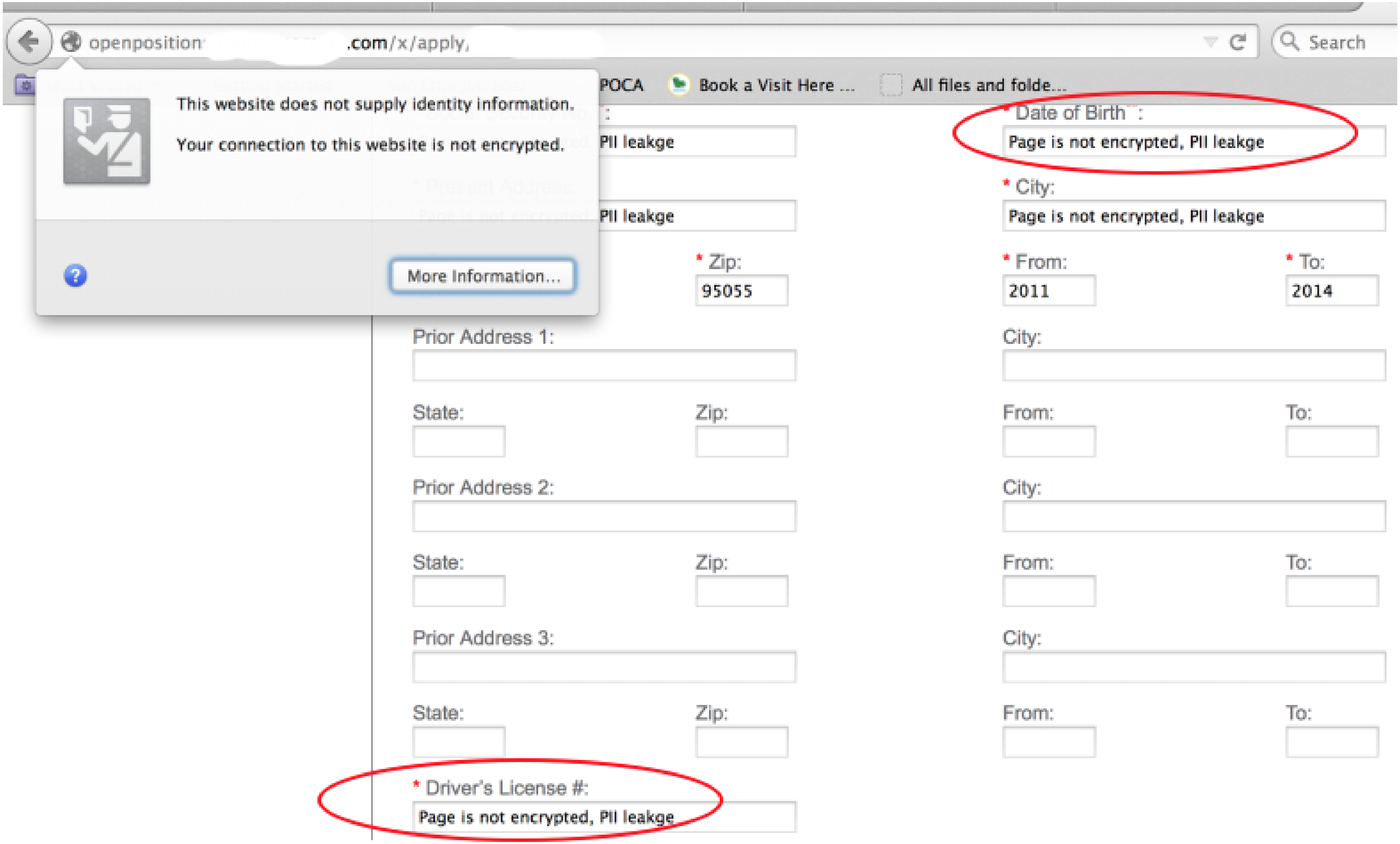
Email “ATS”

- Quick and easy to apply, easy to get lost
- Develop some short of tracking spreadsheetSubject line is important
- Attachment file names are important
- Have a folder & file naming convention in email client & storage
- Relevant cover letter in the body of the email
- Digital signature is a bonus

ATS fails

- Providing references before talking with anyone
- Ensure the ATS you use doesn't require PII/NPPI
  - SSANs in BrassRing
- Test and validate your application process
  - Get a friend to apply, do they make it through the process? Past HR at least?
- Test & validate your promotion efforts
  - Have HR pass every resume
- Avoid the common application fails
  - The initial impressions last

ATS Fails – PII & NPPI & HTTPS



openposition[redacted].com/x/apply,[redacted]

This website does not supply identity information.

Your connection to this website is not encrypted.

* Social Security No.:
Page is not encrypted, PII leakge

* Date of Birth :
Page is not encrypted, PII leakge

* Present Address:
Page is not encrypted, PII leakge

* City:
Page is not encrypted, PII leakge

* Zip:
95055

* From:
2011

* To:
2014

Prior Address 1:

City:

State:

Zip:

From:

To:

Prior Address 2:

City:

State:

Zip:

From:

To:

Prior Address 3:

City:

State:

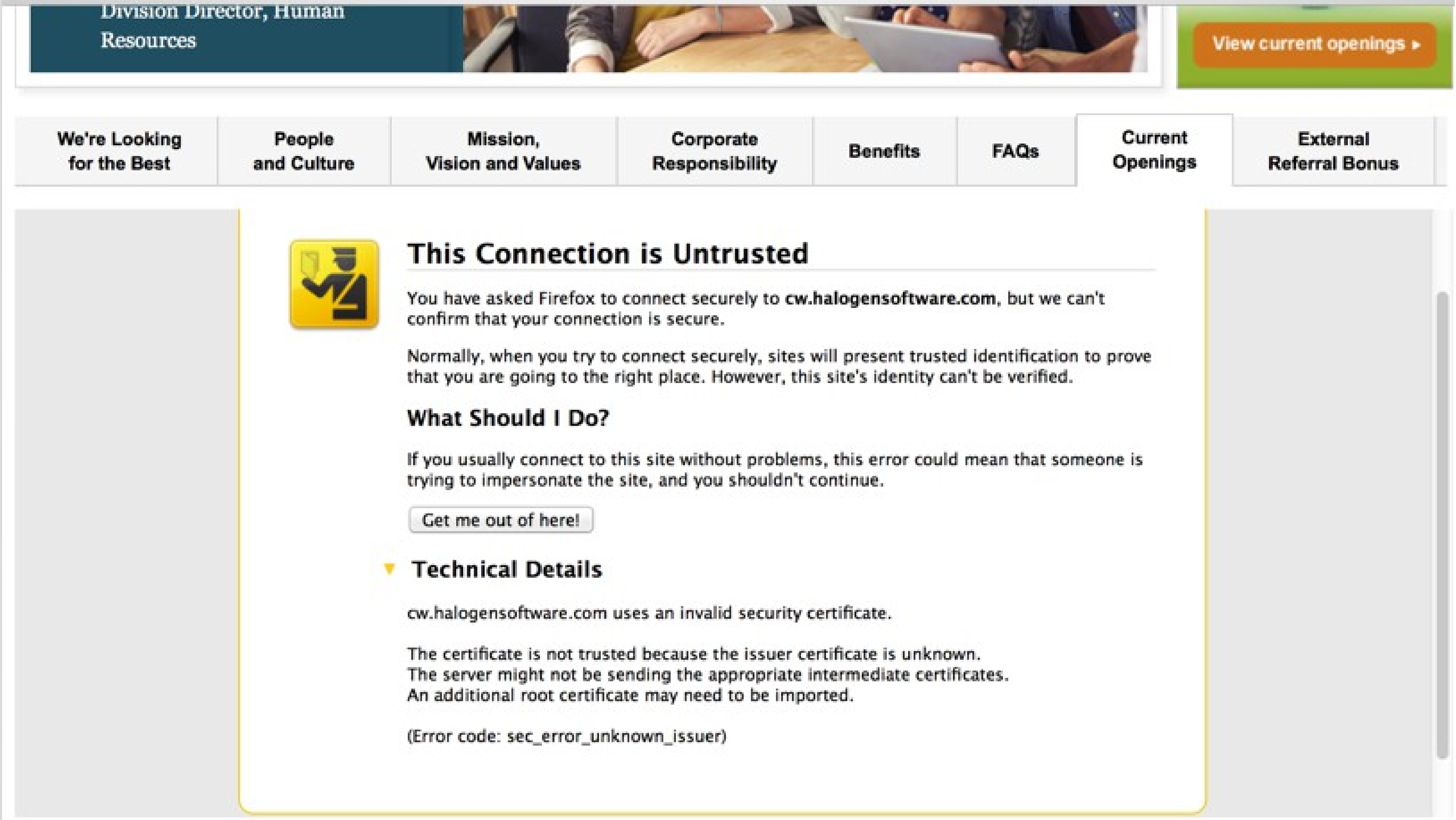
Zip:

From:

To:

* Driver's License #:
Page is not encrypted, PII leakge

ATS Fails – HTTPS & Certificates



This Connection is Untrusted

You have asked Firefox to connect securely to **cw.halogensoftware.com**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

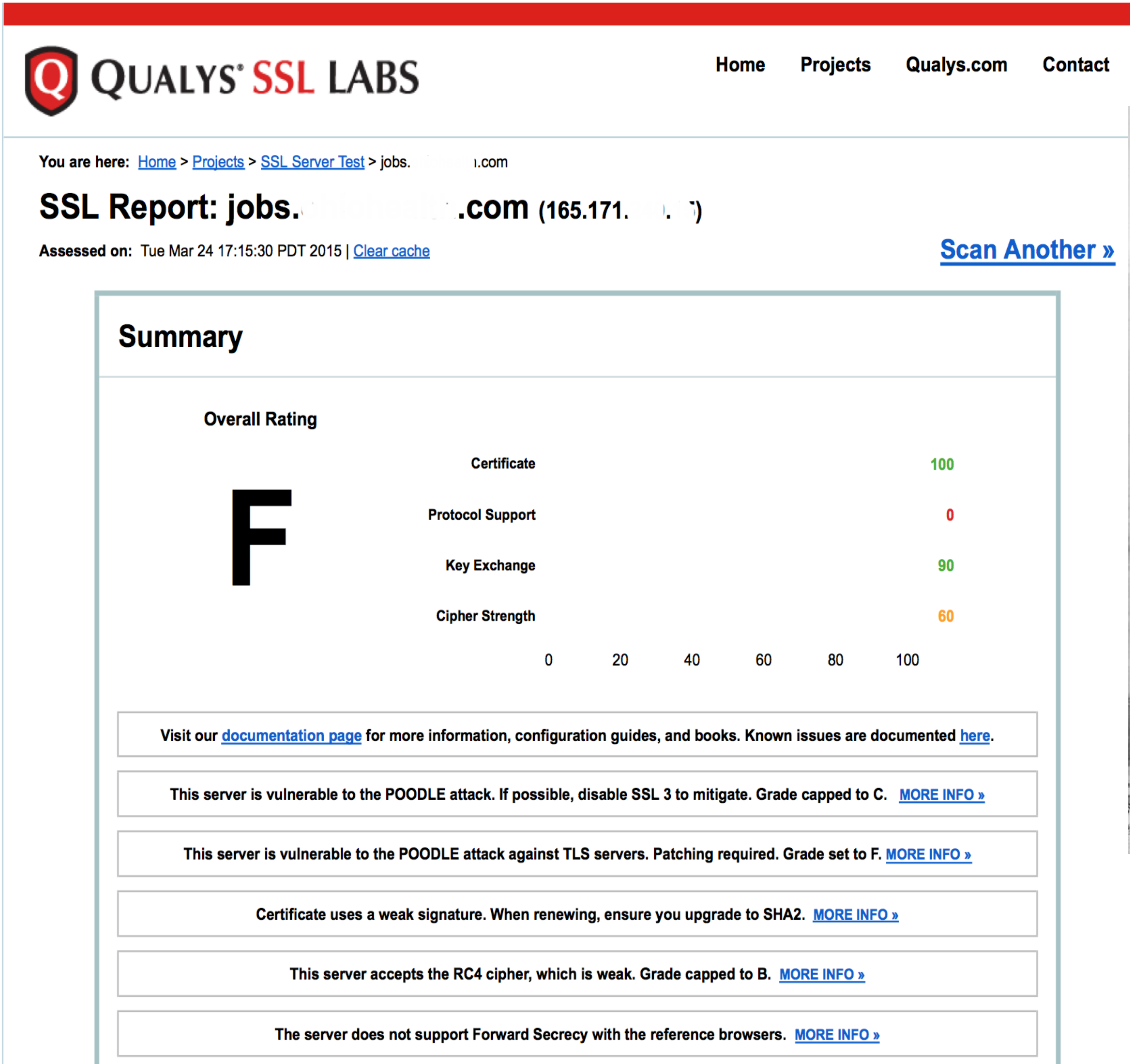
Technical Details

cw.halogensoftware.com uses an invalid security certificate.

The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.

(Error code: sec_error_unknown_issuer)

ATS Fails – HTTPS & Certificates



You are here: Home > Projects > SSL Server Test > jobs.[redacted].com

SSL Report: jobs.[redacted].com (165.171.[redacted])

Assessed on: Tue Mar 24 17:15:30 PDT 2015 | Clear cache

Scan Another »

Summary

Overall Rating

F

Certificate	100
Protocol Support	0
Key Exchange	90
Cipher Strength	60

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

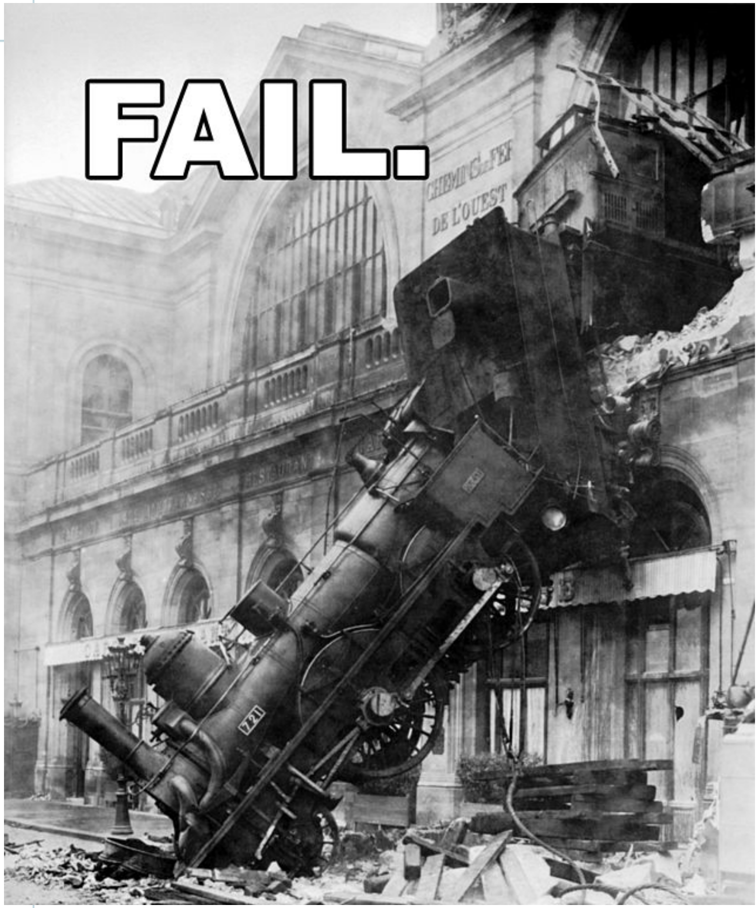
This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. MORE INFO »

This server is vulnerable to the POODLE attack against TLS servers. Patching required. Grade set to F. MORE INFO »

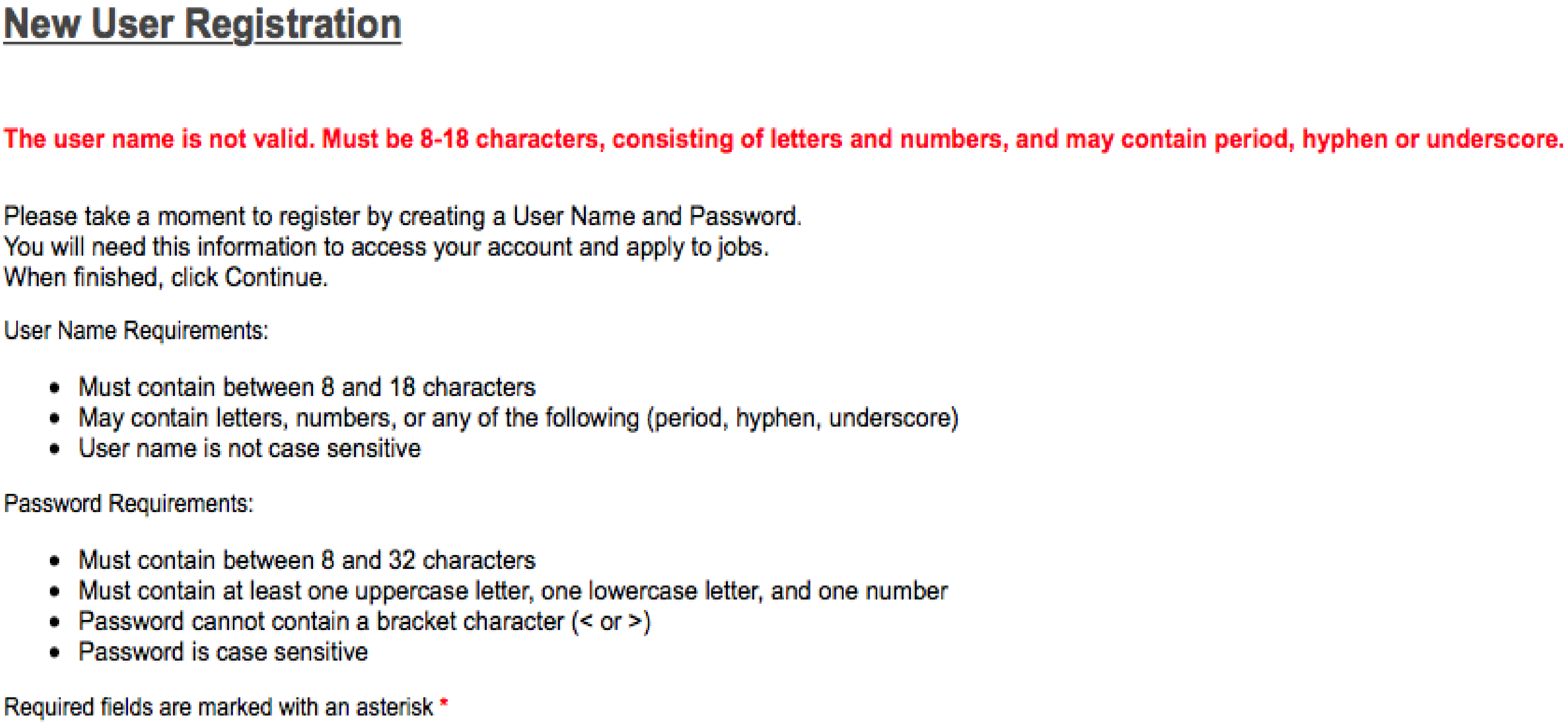
Certificate uses a weak signature. When renewing, ensure you upgrade to SHA2. MORE INFO »

This server accepts the RC4 cipher, which is weak. Grade capped to B. MORE INFO »

The server does not support Forward Secrecy with the reference browsers. MORE INFO »



ATS Fails – User IDs



New User Registration

The user name is not valid. Must be 8-18 characters, consisting of letters and numbers, and may contain period, hyphen or underscore.

Please take a moment to register by creating a User Name and Password.
You will need this information to access your account and apply to jobs.
When finished, click Continue.

User Name Requirements:

- Must contain between 8 and 18 characters
- May contain letters, numbers, or any of the following (period, hyphen, underscore)
- User name is not case sensitive

Password Requirements:

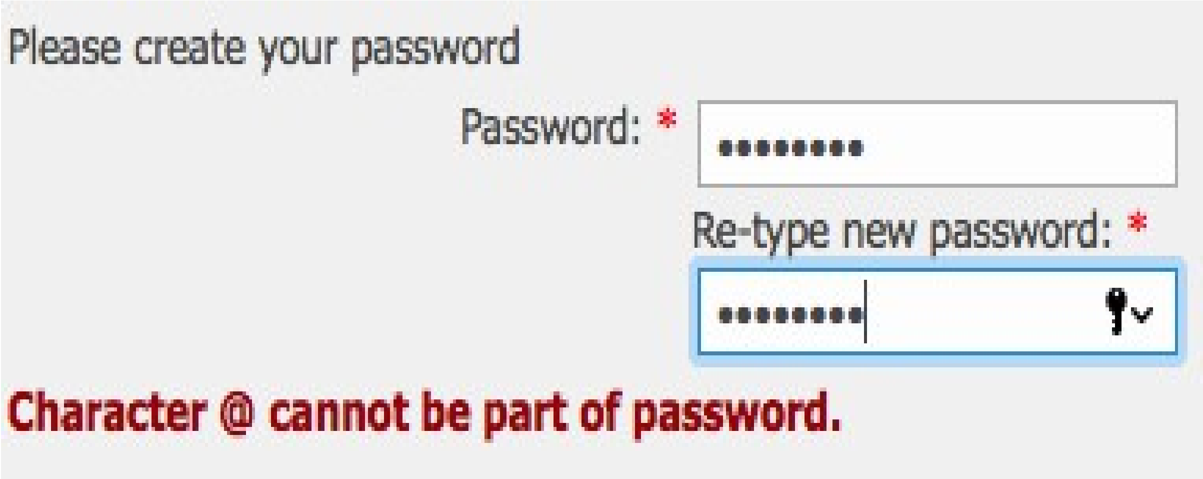
- Must contain between 8 and 32 characters
- Must contain at least one uppercase letter, one lowercase letter, and one number
- Password cannot contain a bracket character (< or >)
- Password is case sensitive

Required fields are marked with an asterisk *

ATS Fails – Passwords

Error: Invalid Data. Review all error messages below to correct your data.

Character @ cannot be part of password.



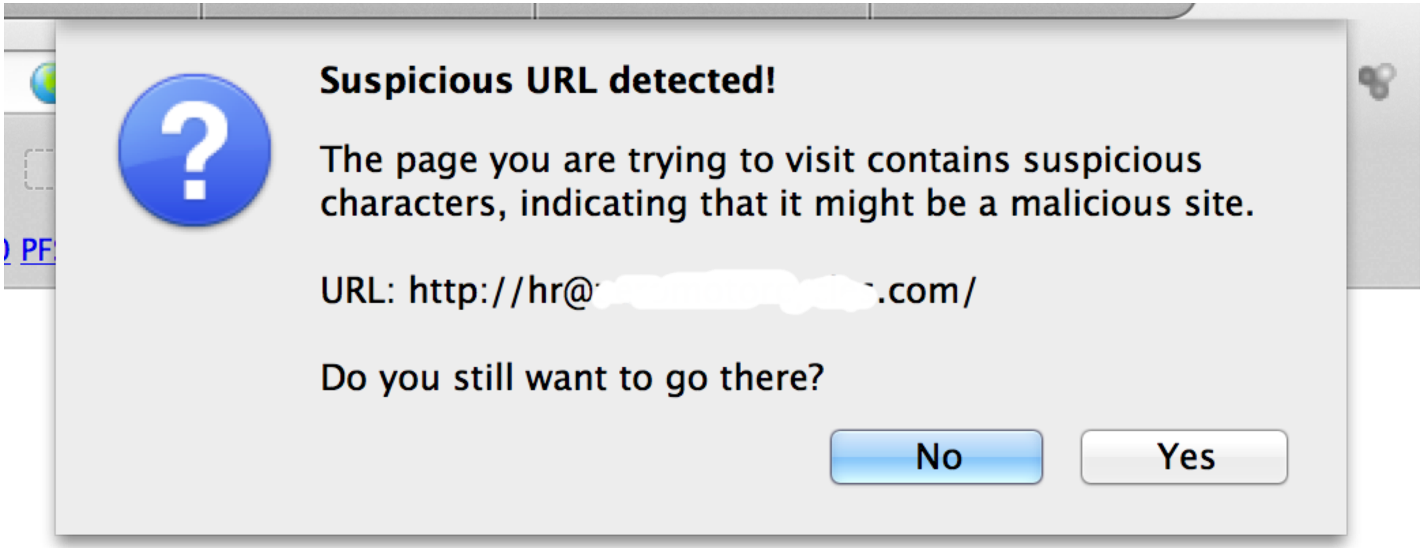
Please create your password

Password: * ●●●●●●●●

Re-type new password: * ●●●●●●●●

Character @ cannot be part of password.

ATS Fails – Bad UX/UI & AppSec

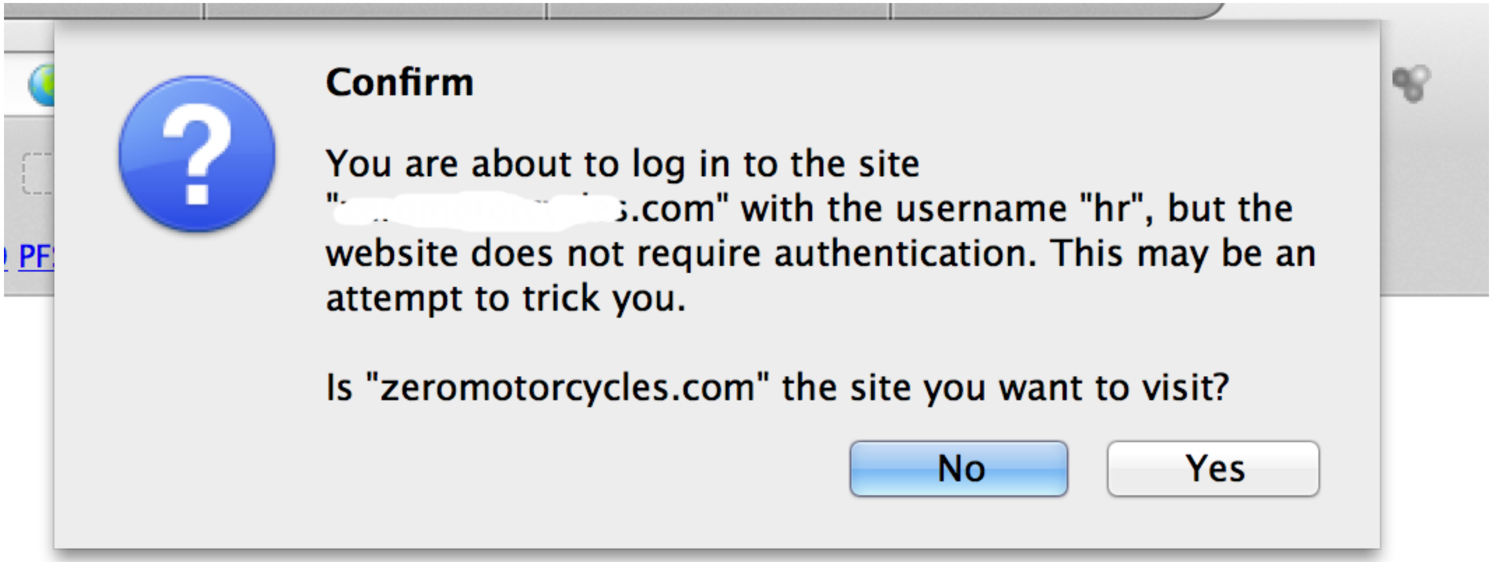


Suspicious URL detected!

The page you are trying to visit contains suspicious characters, indicating that it might be a malicious site.

URL: http://hr@[redacted].com/

Do you still want to go there?

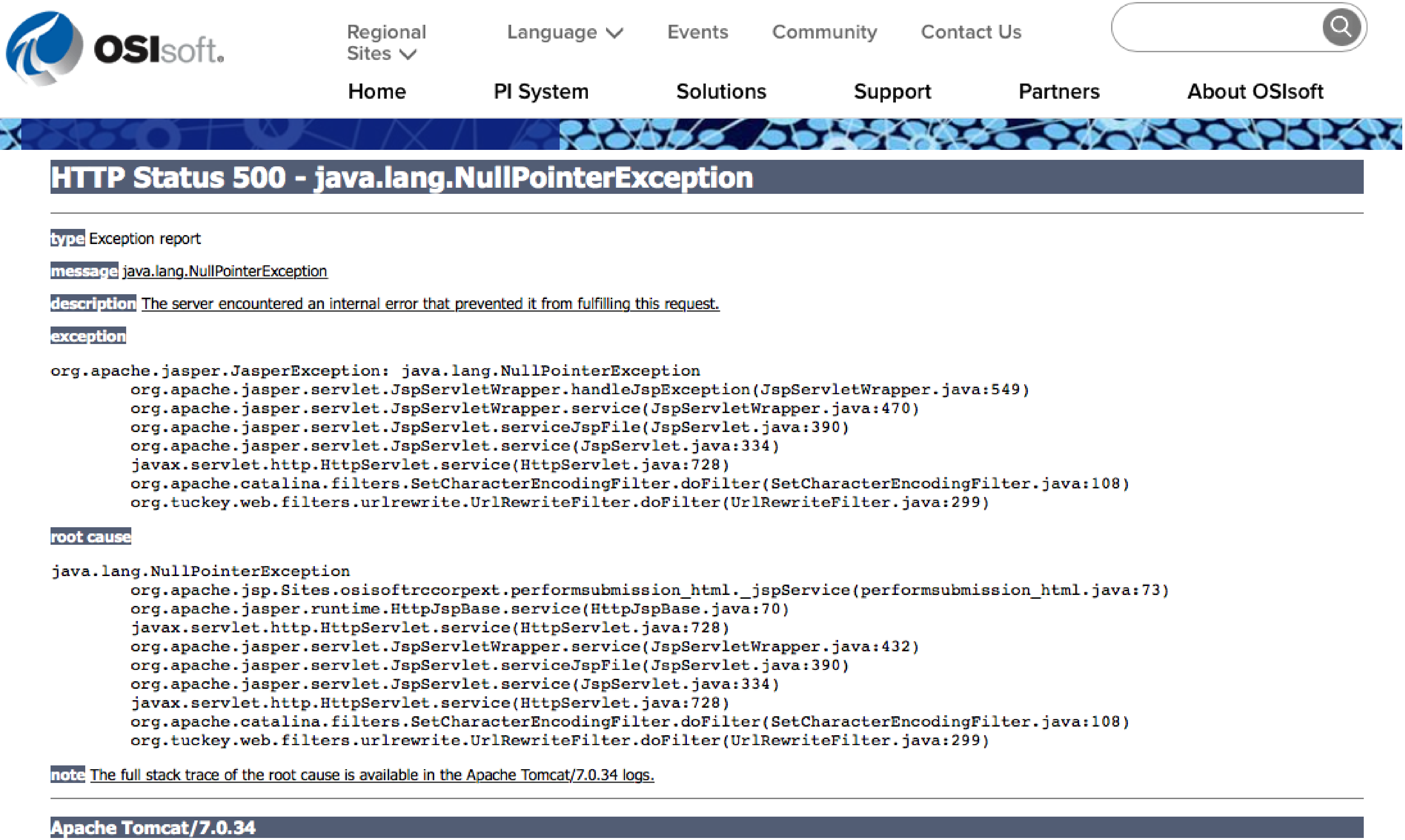


Confirm

You are about to log in to the site "[redacted].com" with the username "hr", but the website does not require authentication. This may be an attempt to trick you.

Is "zeromotorcycles.com" the site you want to visit?

ATS Fails – Bad Error Handling



HTTP Status 500 - java.lang.NullPointerException

type Exception report

message java.lang.NullPointerException

description The server encountered an internal error that prevented it from fulfilling this request.

exception

```
org.apache.jasper.JasperException: java.lang.NullPointerException
	org.apache.jasper.servlet.JspServletWrapper.handleJspException(JspServletWrapper.java:549)
	org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:470)
	org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:390)
	org.apache.jasper.servlet.JspServlet.service(JspServlet.java:334)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:728)
	org.apache.catalina.filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:108)
	org.tuckey.web.filters.urlrewrite.UrlRewriteFilter.doFilter(UrlRewriteFilter.java:299)
```

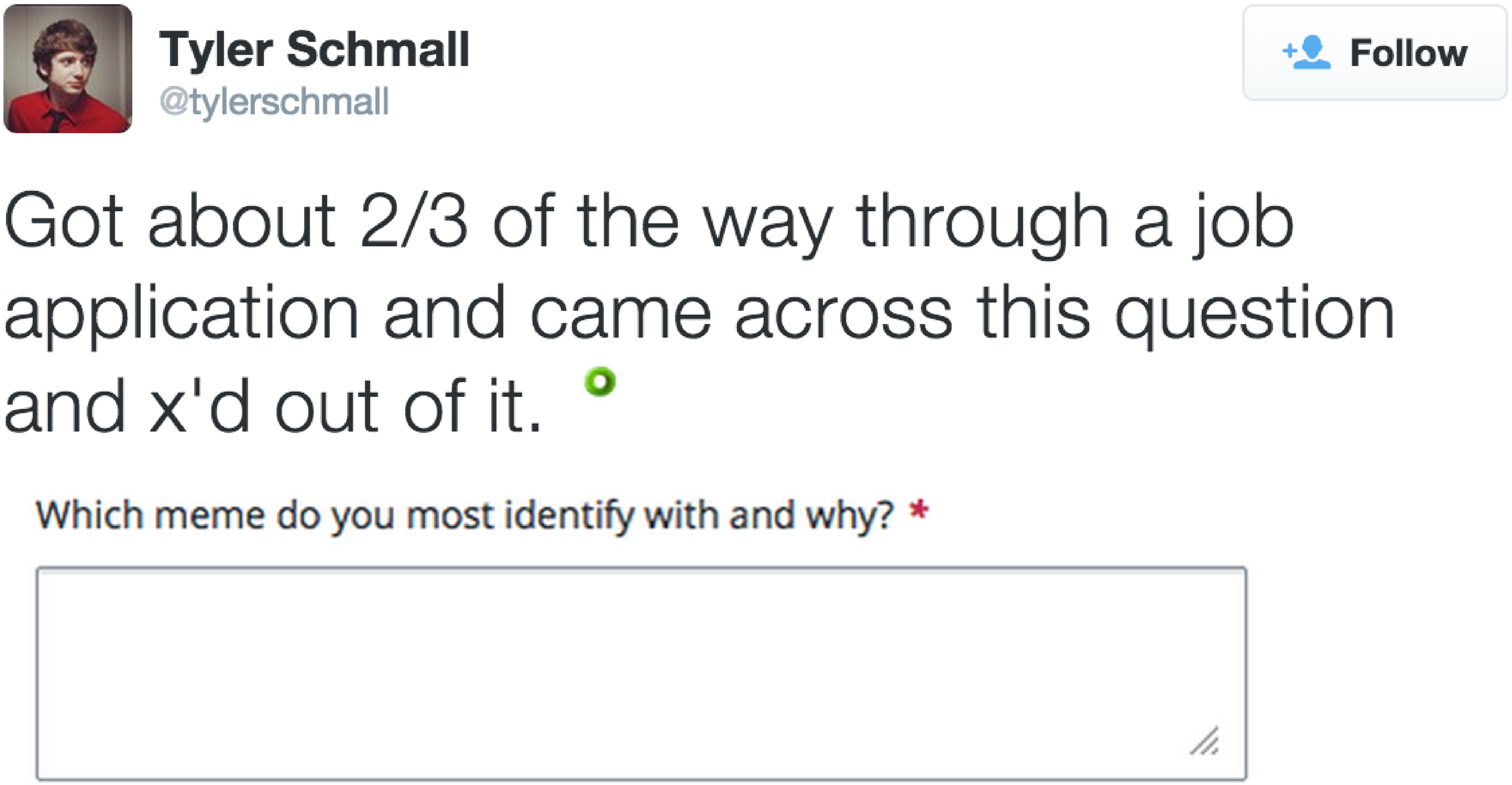
root cause

```
java.lang.NullPointerException
	org.apache.jsp.Sites.osisoftrccorpext.performsubmission_html._jspService(performsubmission_html.java:73)
	org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:728)
	org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:432)
	org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:390)
	org.apache.jasper.servlet.JspServlet.service(JspServlet.java:334)
	javax.servlet.http.HttpServlet.service(HttpServlet.java:728)
	org.apache.catalina.filters.SetCharacterEncodingFilter.doFilter(SetCharacterEncodingFilter.java:108)
	org.tuckey.web.filters.urlrewrite.UrlRewriteFilter.doFilter(UrlRewriteFilter.java:299)
```

note The full stack trace of the root cause is available in the Apache Tomcat/7.0.34 logs.

Apache Tomcat/7.0.34

The Badass Owl



Tyler Schmall
@tylerschmall

Got about 2/3 of the way through a job application and came across this question and x'd out of it.

Which meme do you most identify with and why? *

THE FAILBOAT
HAS ARRIVED

Build The Relationship

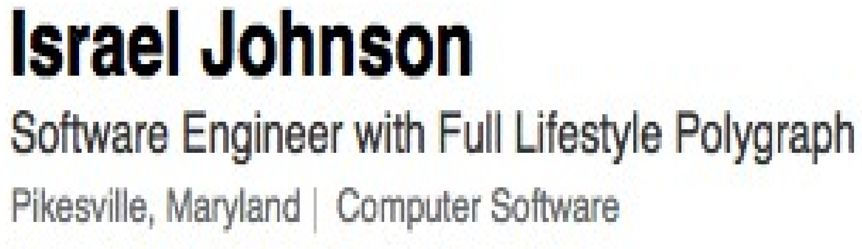
- Using the ATS and working with your recruiter takes time & communications
    - All worthwhile
    - Have your recruiter join you in interviews
    - Have them on your InfoSec awareness distro listings
    - Invite them to your team training events & brown bags
    - Explain why or why not on candidates
        - If not for this role, perhaps a future one?

Resume Review

- Candidate interested in the role?
- Can they learn the topics & technology not listed?
- Security clearance listed?
- File Metadata
- Did they submit a cover letter?

    Why did the job, the company sound interesting?

    What info not on resume?



Israel Johnson

Software Engineer with Full Lifestyle Polygraph

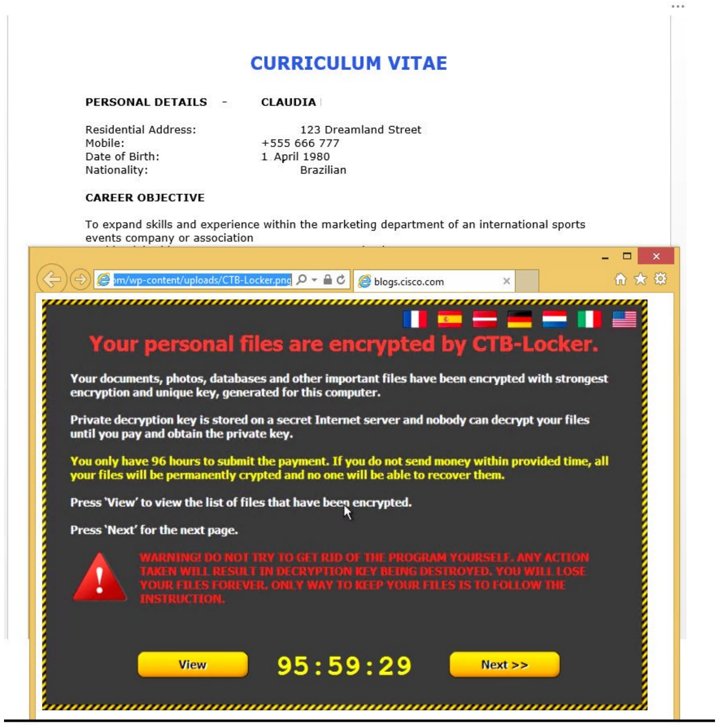
Pikesville, Maryland | Computer Software

Security Clearances

- Do not belong on the resume or social media profiles
- Broadcasting makes you a bigger target and look unprofessional
- DSS/OPM does not look kindly on this
  - Read the NDA you signed
  - Does not matter that the APT$ stole it all
- When asked by HR/recruitment, the proper answer: “That information can be verified with a conversation with your Personal Security Officer.”
  - Your HR should know this, and handle without questioning integrity
  - If this answer is not satisfactory, do you want to work for them?

Resume Attacks

- Virus scan/sandbox resumes
  - Malware/malicious code
  - Trackers



CURRICULUM VITAE

PERSONAL DETAILS - CLAUDIA

Residential Address: 123 Dreamland Street
Mobile: +555 666 777
Date of Birth: 1 April 1980
Nationality: Brazilian

CAREER OBJECTIVE

To expand skills and experience within the marketing department of an international sports events company or association

Your personal files are encrypted by CTB-Locker.

Your documents, photos, databases and other important files have been encrypted with strongest encryption and unique key, generated for this computer.

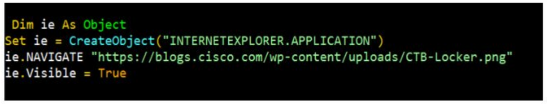
Private decryption key is stored on a secret Internet server and nobody can decrypt your files until you pay and obtain the private key.

You only have 96 hours to submit the payment. If you do not send money within provided time, all your files will be permanently crypted and no one will be able to recover them.

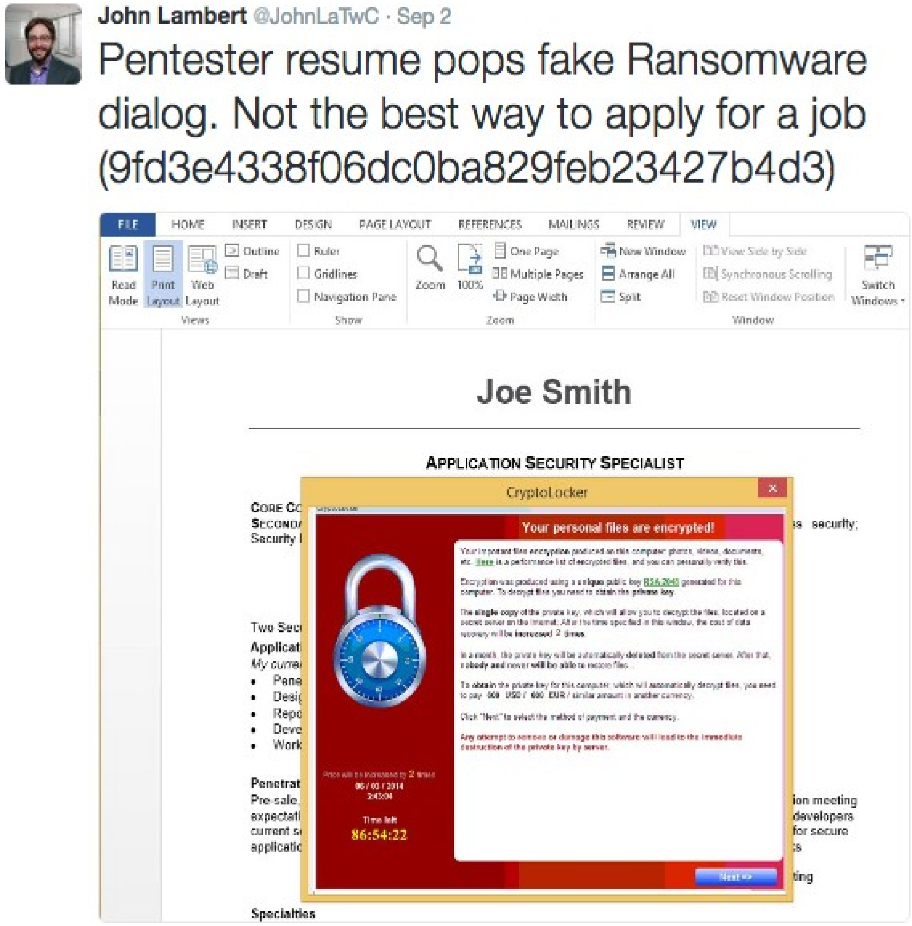
Press 'View' to view the list of files that have been encrypted.

Press 'Next' for the next page.

WARNING! DO NOT TRY TO GET RID OF THE PROGRAM YOURSELF. ANY ACTION TAKEN WILL RESULT IN DECRYPTION KEY BEING DESTROYED. YOU WILL LOSE YOUR FILES FOREVER. ONLY WAY TO KEEP YOUR FILES IS TO FOLLOW THE INSTRUCTION.



```
 Dim ie As Object
Set ie = CreateObject("INTERNETEXPLORER.APPLICATION")
ie.NAVIGATE "https://blogs.cisco.com/wp-content/uploads/CTB-Locker.png"
ie.Visible = True
```



John Lambert @JohnLaTwC · Sep 2

Pentester resume pops fake Ransomware dialog. Not the best way to apply for a job (9fd3e4338f06dc0ba829feb23427b4d3)

Joe Smith

APPLICATION SECURITY SPECIALIST

CORE CO
SECONDA
Security
s security;

Two Sec
Applicat
My curre
- Pene
- Desi
- Repo
- Deve
- Work

Penetrat
Pre-sale
expectati
current s
applicati
ion meeting
developers
for secure
s
ting

Specialties

CryptoLocker

Your personal files are encrypted!

Your important files encryption produced on this computer: photos, videos, documents, etc. Here is a complete list of encrypted files, and you can personally verify this.

Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.

The single copy of the private key, which will allow you to decrypt the files, located on a secret server on the Internet. After the time specified in this window, the cost of data recovery will be increased 2 times.

In a month, the private key will be automatically deleted from the secret server. After that, nobody and never will be able to restore files.

To obtain the private key for this computer, which will automatically decrypt files, you need to pay 300 USD / 300 EUR / similar amount in another currency.

Click "Next" to select the method of payment and the currency.

Any attempt to remove or damage this software will lead to the immediate destruction of the private key by server.

Price will be increased by 2 times
06 / 03 / 2014
3:45:04

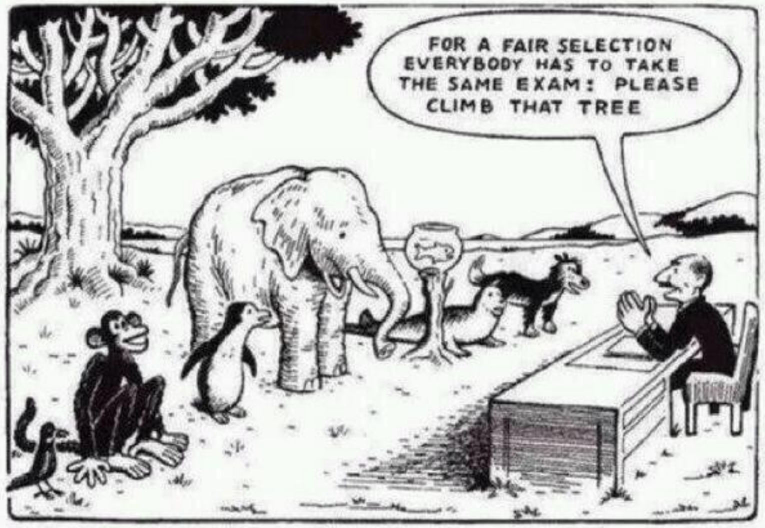
Time left
86:54:22

Core Problem aka Opportunity #3

THE INTERVIEW

Vetting the candidate

The interview process is hard. But when you compound that with the nervousness of trying to get a job in your “dream field” and the fact that most of us are weird shits who do weird shit during the day, the interview can be anxiety-inducing. There are a lot of little things that can be done to make it a little bit less awful.


FOR A FAIR SELECTION EVERYBODY HAS TO TAKE THE SAME EXAM: PLEASE CLIMB THAT TREE

Our Education System

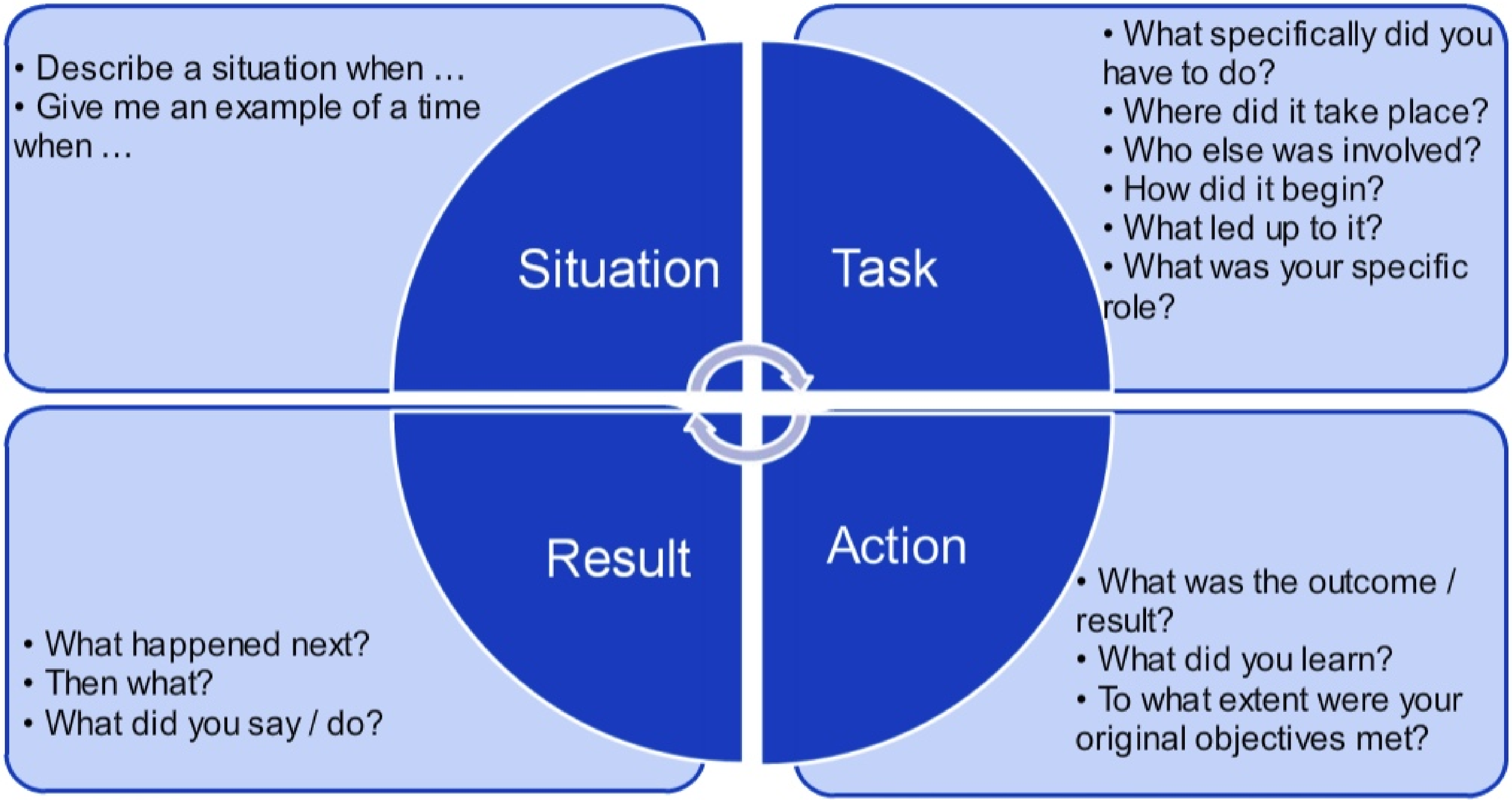
“Everybody is a genius. But if you judge a fish by its ability to climb a tree, it will live its whole life believing that it is stupid.”

- Albert Einstein

Pre-interview

- Consider who you want & need to interview candidates
  - Candidates do not want to be interviewed by a person who has no understanding of the job
- Consider the types of and specific questions you want to ask **before** the interview process
  - Respect the sensitivities of the applicants in your questions
    - Know the no-no questions/topics, the “illegal” ones
    - NDA/Clearances
  - The series should reflect the requirements of the PD
    - Which should reflect the daily duties of the role
    - Leverage the Situation – Task – Action – Result (STAR) method
    - Eliminate the juvenile and pointless interview questions

Situation – Task – Action – Result (STAR)



Situation

- Describe a situation when …
- Give me an example of a time when …

Task

- What specifically did you have to do?
- Where did it take place?
- Who else was involved?
- How did it begin?
- What led up to it?
- What was your specific role?

Result

- What happened next?
- Then what?
- What did you say / do?

Action

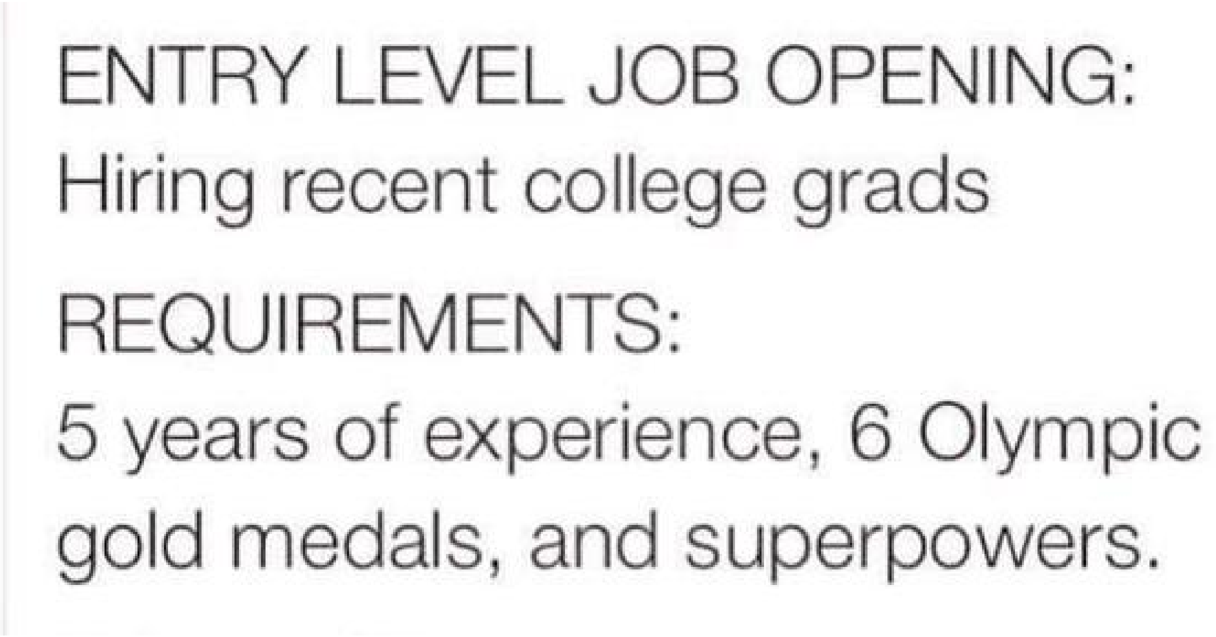
- What was the outcome / result?
- What did you learn?
- To what extent were your original objectives met?

Dealing with volunteered information

- Some candidates will volunteer information that you would prefer not to know
- The optimal way to handle the situation is to not pursue it, nor make note of it
- You may be unable to erase the information from your memory, but you can eliminate it as a discussion point and selection factor

Define Key Areas

- How do you define key areas/topics?
- Testing/evaluating for specific skills? Or more General?
- How do you match up skills to the position description (PD), then the areas to question per candidate?



ENTRY LEVEL JOB OPENING:

Hiring recent college grads

REQUIREMENTS:

5 years of experience, 6 Olympic gold medals, and superpowers.

Timing And Travel

- Work with your scheduler on timing
  - Secure a conference room for phone screens vs your desk
  - If candidate is on site overlaps lunchtime, treat them
  - Avoid having candidates waiting for hours in conference rooms
  - If you are unable to organize interviews properly, we can assume the poor organization skills are prevalent
- Reimburse for travel expenses
- Showing respect for time and investment, treating like a human being goes a long way

Prepare For Your Review

- Review review web sites (Glassdoor, Indeed, Yelp, Google, etc.) for potential questions on your company & culture
  - Have answers/commentary for candidates
  - Note if candidates do not ask about these topics

ACTUALLY, IT IS ABOUT ETHICS
IN JOB INTERVIEWS
memegenerator.net

Question planning

- Creating the interviews

    Balancing fact based questions vs essay/short

- Does your interview team share questions?

    Figure out who asks what

    Avoid duplication – or do you?

- Avoid using the question lists found online verbatim
- We need to be real in job interviews
    - The real projects and problems your team is struggling with

Questioning the Candidate - Do

- Guide the interview
- Interrupt tactfully to keep the candidate focused
- Use silence to give candidate time to gather their thoughts, or for you to consult their resume or your notes

- Use open questions to probe for more details, ask the candidate to explain in detail
  - Consider NDAs
- Seek clarification of vague statements & jargon
  - Consider NDAs
- Seek clarification if the candidate uses ‘we’ instead of ‘I’

Questioning the Candidate - Don’t

- Ask leading or hypothetical questions
- Use closed questions other than to confirm candidate responses
- ‘Interrogate’ the candidate

- Waste time with preambles and justifications for questions
- Steal the limelight from the candidate
- Let your moods or emotions lead the interview
- Exhibit annoying body language or fidget

Puzzles & PCAPs

- Some hiring managers swear by using a hack site or PCAP exercise for initial vetting
  - Good way to see a candidates attention to detail, report writing, technical & research abilities
  - Conduct after an initial interview/phone screen
- What is the ROI for a candidate to accomplish?
- How is the exercise relating to your operations, your tools?
- How is it reflective to the work for this role?
- How is it reflective of your business environment?

Stump The Monkey

- “Stump the monkey” isn’t fun for anyone
  - Trick questions, the Google stumpers
  - Does not convey how good of an analyst/engineer/hacker they are or could be
- Objective is to assess how does the candidate processes information to mitigate the threat/risk/vulnerability
  - Not how fast they can recite knowledge
- This approach could dissuade a good candidate from accepting an offer

Lasting Impressions

- The intent is to find individuals for your team, not prove how smart you are - or how dumb they are
  - Lasting impression on you & company
  - See the interview ratings & feedback (Glassdoor/Indeed)
  - Sometimes there is more than one answer
    - With the answer different than yours
- Be respectful of your candidates
  - Gives you a better read on each person’s worldview and thought process
  - Builds a relationship between you and the candidate — the very things you want
- See Wheaton's law

29 July

http://dontbeadickday.com/

Question Bias

- So what if the candidate does not know how to work with oak

  Can they learn to work with mahogany?
- Avoid close-ended questions

  “Have you worked with teak”?

  “What is the UDP flag on a DNS request that fails?”

  “What protocol uses port 0?”

Toolset Bias

- InfoSec is more than tool = problem
- Best to use situational, exploratory conversations

  What are some of the ways you have used wood to address vulnerabilities?

  Not: Have you ever used maple wood?
- Review: If Carpenters Were Hired Like Programmers

Hiring Bias

- Stop passing judgment
  - Piercings and tattoos no longer mean that they're ex-convicts
- See Wheaton's Law
- People get nervous and forget things
  - How would they figure it out?
- So what if they self-identify as a hacker?
  - Superpowers for good or for evil?
- Review: Evaluate the Scrapper

Time In A Role

- Why does the length of time in a role matter?
- Most are out of the candidate's control
    - Startups, Company failure or change of direction
    - Contract work
        - Business climate pushing the use of contractors & consultants
            - To the detriment of everyone except recruiter
    - Layoff, unemployment
- Why this concern on “job hopping”?
- This notion of lifetime employment is antiquated and false
    - Tour of duty employment
- Put yourself in their place, adjust our paradigm & expectations

Periods Of Unemployment

- Unemployment does not mean untouchable
  - Put aside your bias
  - Listen to the reason(s)
    - Don’t assume they’re excuses
- Discrimination
- Put yourself in their place

Time Between Roles

- Not all gaps between jobs should be a (bad) reflection on the candidate

    Family illnesses

    School, personal development

    Recession (yes, places have never recovered)

    Personal time, recuperation from last role

    Toxic work environment/manager

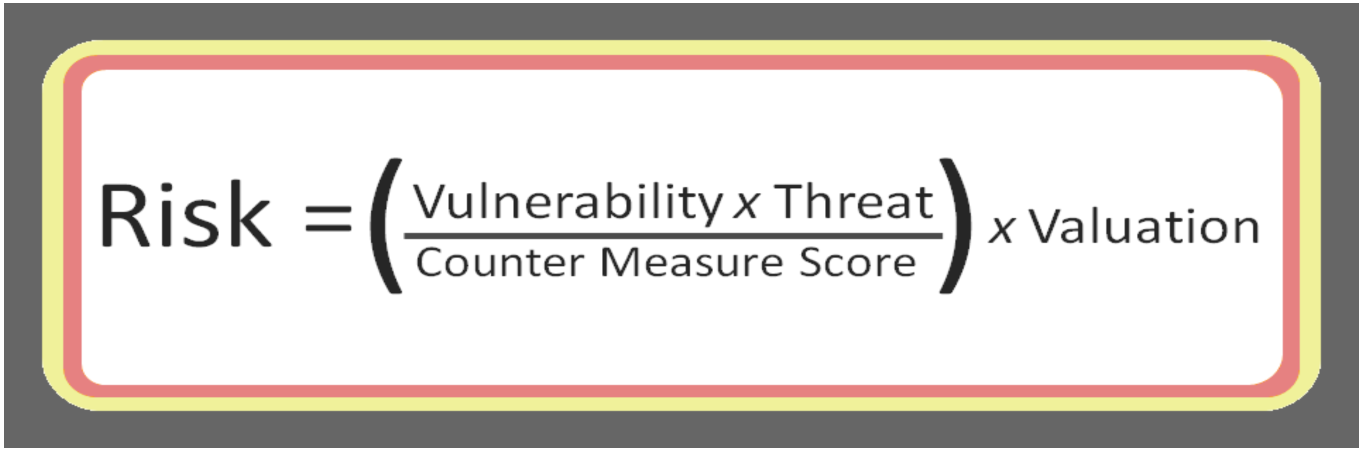
    “Mourning period” or sabbatical after getting laid off from a job/company they really enjoyed being a part of (or needed)

The InfoSec Question

- Can the candidate explain how you can reduce Risk by affecting Vulnerability, Threat, Asset or Cost?

  Generally, most technical folk focus on Vulnerability.

  Most nontechnical/inexperienced folk focus on Threat
- We need to reduce Vulnerability and Threat, but also work within Cost



$$\text{Risk} = \left(\frac{\text{Vulnerability} \times \text{Threat}}{\text{Counter Measure Score}}\right) \times \text{Valuation}$$

The Trifecta

- Ability to learn; with the want & desire to learn
- Passion

    What is this person passionate about?

    Learning? Figuring things out? Solving problems? That is huge.
- Ability to be wrong/fail, and to do so well.

    We will all fail.

    Can you learn and grow from it, or do you hide it and try to blame others?

Hiring Excuses

Commonly heard excuses:

“Not technical enough”

“Not a cultural fit”

In your team interviews, use a scoring system and average the scores to help eliminate bias.

We need to stop using culture fit as a crutch for not hiring someone.

Remember: People are hired for aptitude.

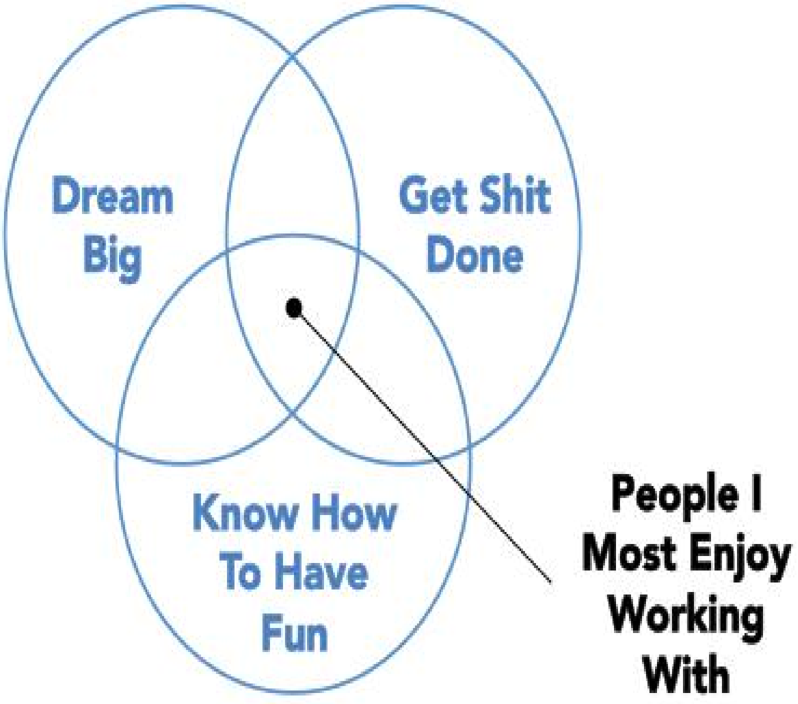
Culture Fit

- Think about whether you would want to work with this individual, but do not use it as an excuse when someone ”better” comes along.
- Do you think the person can do the job?

  Or can they learn to do the job?

  Be an asset to your team?
- Diversity of the team

  a good thing.

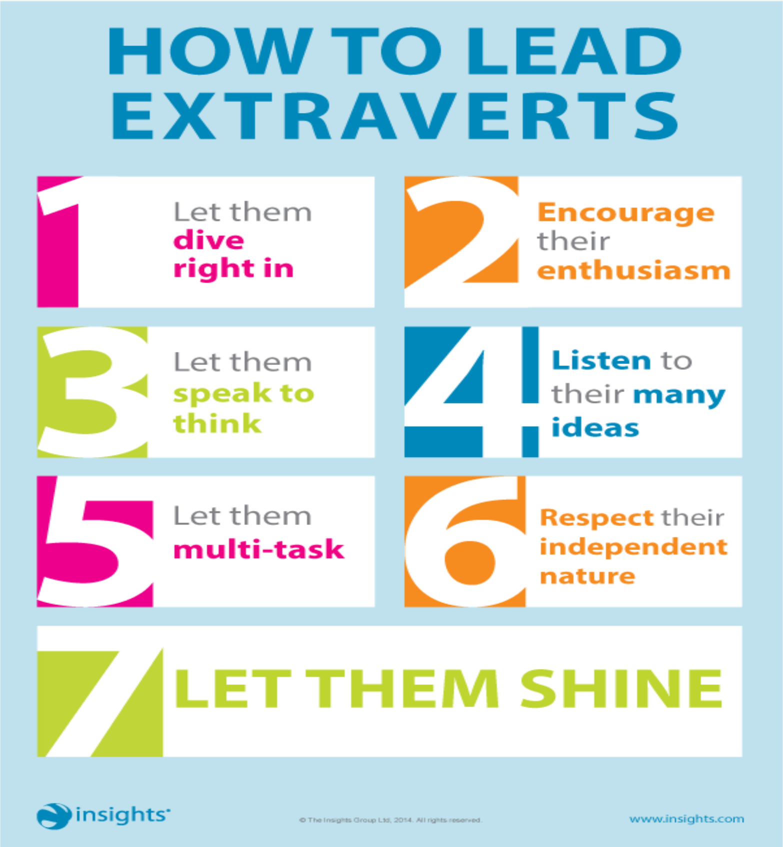


Recruiters call the perfect candidate the “purple squirrel”

Even more rare is the plaid unicorn

Diversity

Some folks are extroverted, some are introverted - some roles align to one or the other. Diversity of our teams are a good thing - diversity in culture, gender, nature, and perspective. That diversity when used effectively can be a godsend in finding the bad actors and working with the business



HOW TO LEAD EXTRAVERTS

1 Let them dive right in

2 Encourage their enthusiasm

3 Let them speak to think

4 Listen to their many ideas

5 Let them multi-task

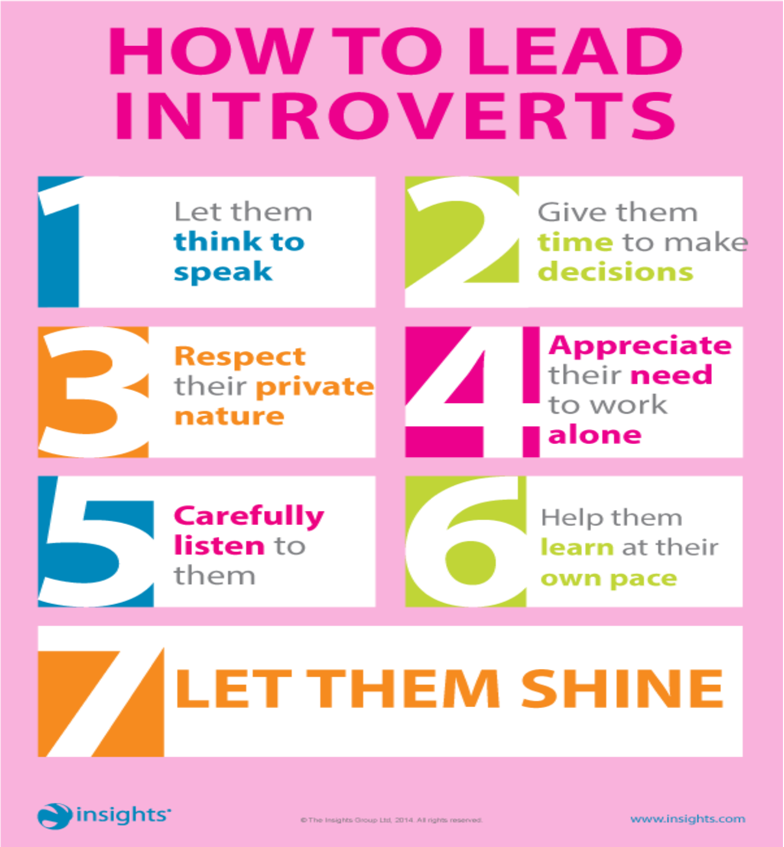
6 Respect their independent nature

7 LET THEM SHINE

insights

© The Insights Group Ltd, 2014. All rights reserved.

www.insights.com



HOW TO LEAD INTROVERTS

1 Let them think to speak

2 Give them time to make decisions

3 Respect their private nature

4 Appreciate their need to work alone

5 Carefully listen to them

6 Help them learn at their own pace

7 LET THEM SHINE

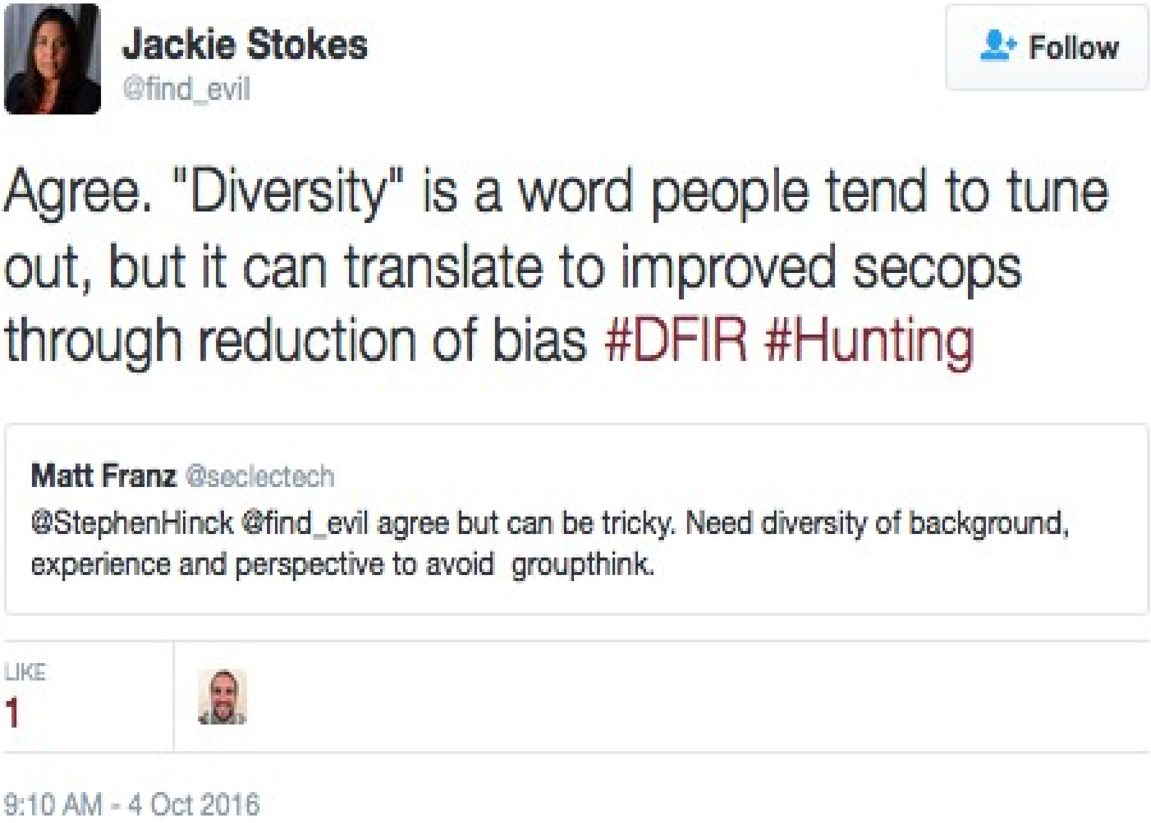
insights

© The Insights Group Ltd, 2014. All rights reserved.

www.insights.com

Diversity

- Diversity of our teams are a good thing
  - Diversity in culture, gender, nature, and perspective.
- That diversity when used effectively can be a godsend in finding the bad actors and working with the business
  - Avoid groupthink



Jackie Stokes
@find_evil

Agree. "Diversity" is a word people tend to tune out, but it can translate to improved secops through reduction of bias #DFIR #Hunting

Matt Franz @seclectech
@StephenHinck @find_evil agree but can be tricky. Need diversity of background, experience and perspective to avoid groupthink.

LIKE
1

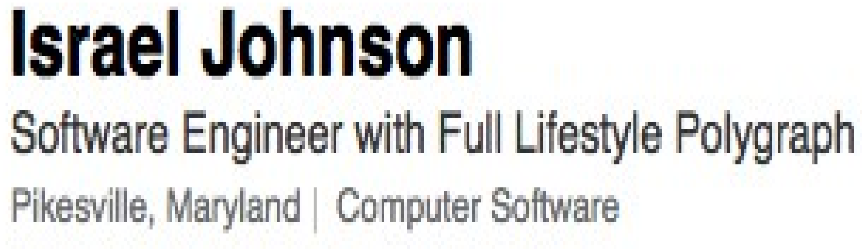
9:10 AM - 4 Oct 2016

Social Interactions

- Are you able to sell the role & the team/company?
- Do your values align with theirs?
- Are they really interested in your product and team?
- If they don't know a question, how would they figure it out? (and Google is down)
- Do they call out interviewers regarding inappropriate questions?
- Do they ask questions? Anything other than found online?
- Check manners with everyone they interacted with
  - Parking staff, reception, physical security

Full Picture

- OSINT on serious candidates
  - GTFG name, email address, domain names
  - Registration information on domains/Ips
  - Social media profiles, blogging sites
  - Inquire your peer network



Israel Johnson

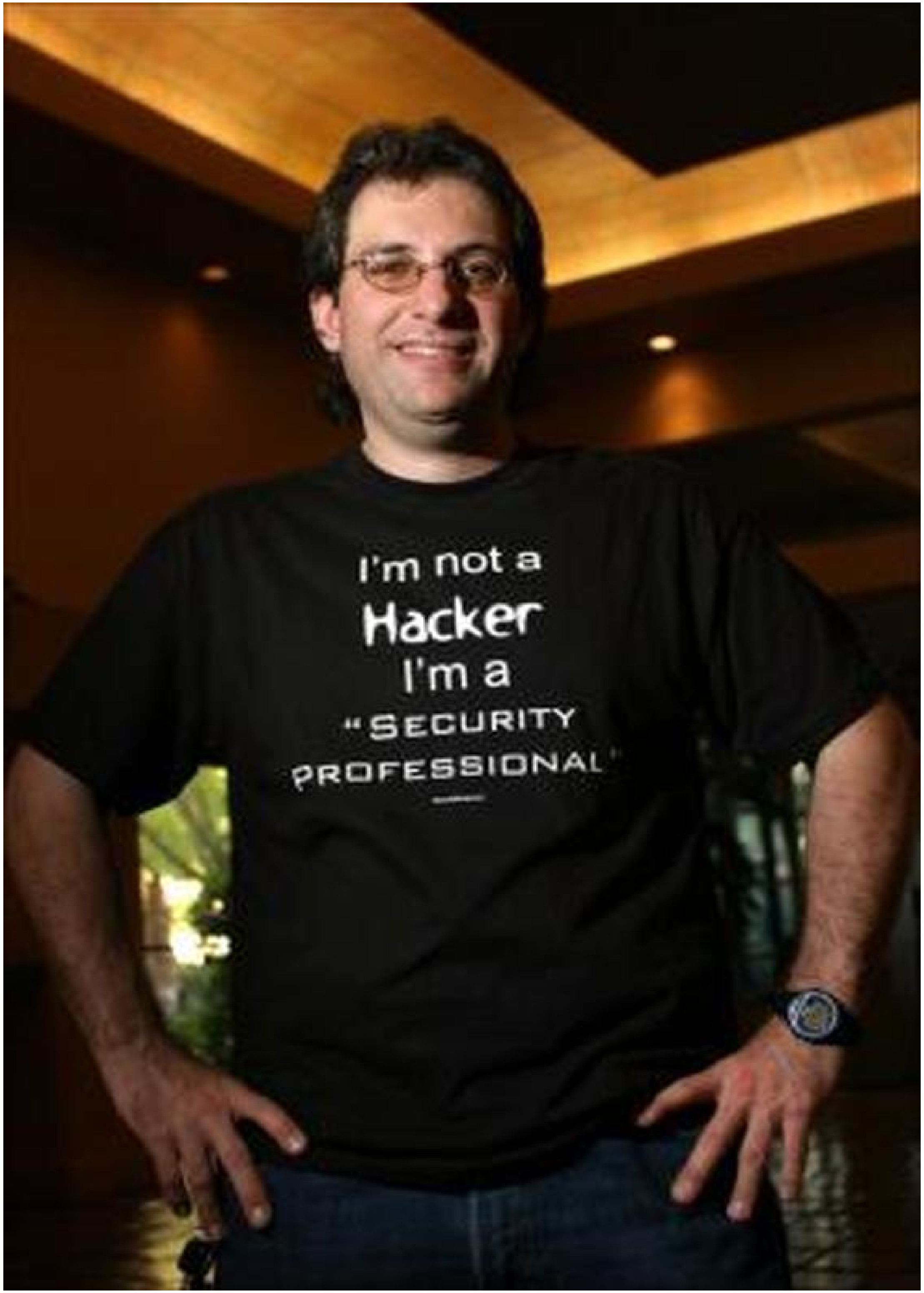
Software Engineer with Full Lifestyle Polygraph

Pikesville, Maryland | Computer Software

Are They Qualified?

- Can they do the tasks listed in the job description?
- Can they learn the tasks in the job description?
- Does their diversity and/or background add to your team?
- Can they answer the InfoSec question?
- Do they have the trifecta?
- It is NOT the job of the ATS or HR to determine if the candidates are qualified.

Closing The Deal



Post-Interview

Managers can not seem to find the balance between being aloof about not getting the job, while botching the opportunity to provide an offer.

Candidates can act like overly attached girlfriend in trying to get any sort of feedback.

Post-Interview Etiquette

- Don’t leave people hanging
- Send an email or call with status updates
  - Contact within 3-4 weeks at maximum
- Provide feedback if they ask
  - If HR/Legal will allow
  - If not, circle back at a later date
- Builds relationships within the community
  - Helps improve the pool of candidates

Provide Feedback

- Glaring resume issues/errors
- Topics to review
  - Tools, Techniques, Procedures (TTPs)
  - Protocols
- Interview tips
  - Talk more/don’t talk as much
  - Etiquette
- Get feedback from them on the process and experience
  - Use this feedback to improve your efforts and processes

Candidate Followup

- Did they send any thank you email/cards?
- Social media requests?

    Creepy

    Question of boundaries

- Did they leave feedback on Glassdoor or elsewhere?

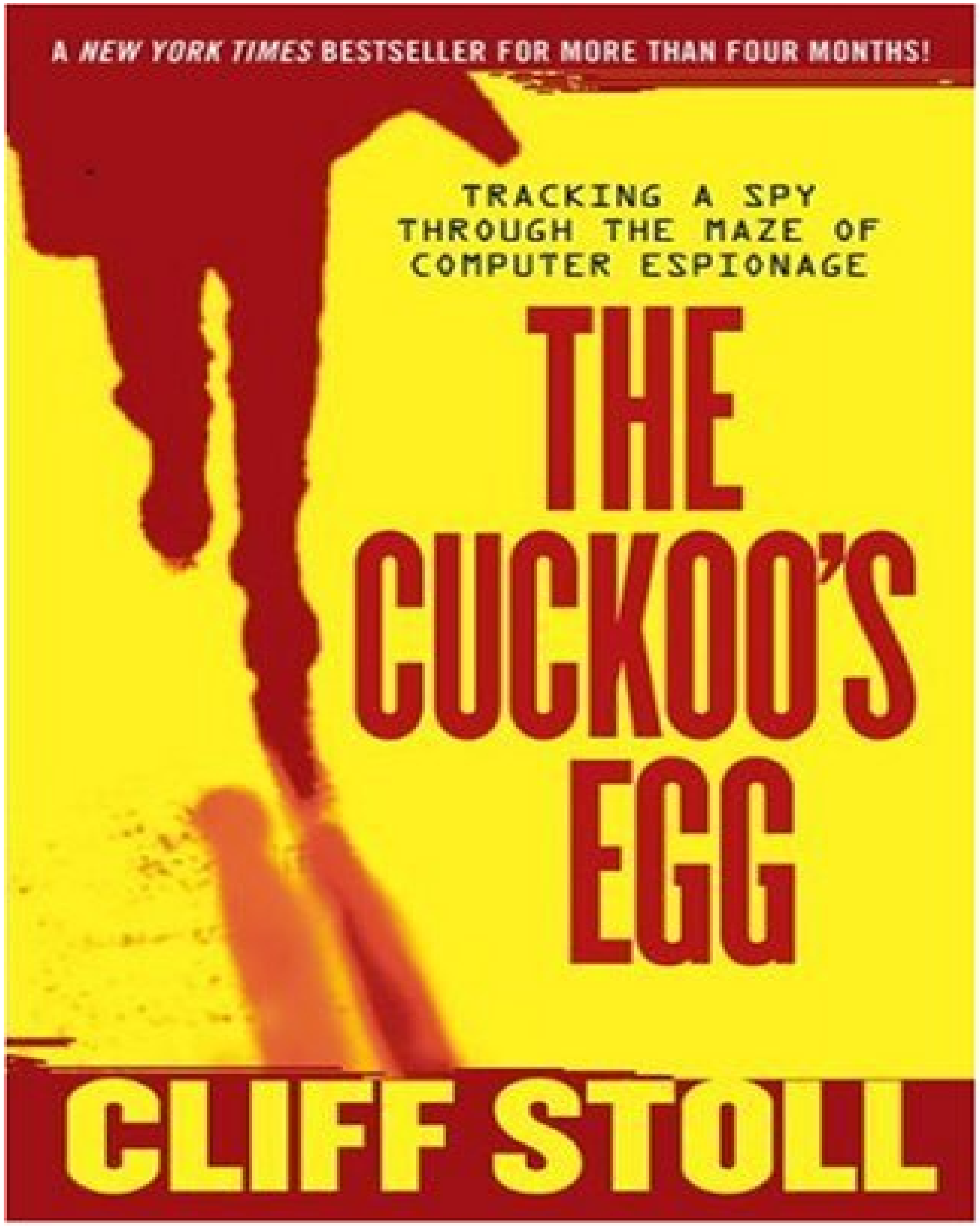
Providing the Offer

- Pay what they are worth
    - Ladies, do not sell yourself short.
    - Managers, don’t be a cheapskate.
    - If you are advertising the role nationwide, you best be paying nationwide rate.
    - Just because it is “cheaper” to live in BFE does not mean you should offer a pay cut.
    - Make it up in other ways
        - PTO, conferences, training budget, gear for the home lab, WFH/work remote, etc

Providing the Offer

- Do not bait and switch
  - Back down from an agreed-upon salary target or position/title when the job offer arrives

Perspective & Expectations


A NEW YORK TIMES BESTSELLER FOR MORE THAN FOUR MONTHS!
TRACKING A SPY THROUGH THE MAZE OF COMPUTER ESPIONAGE
THE CUCKOO'S EGG
CLIFF STOLL

Perspective

- Over all this, how can we make it better?
- How can we keep perspective?

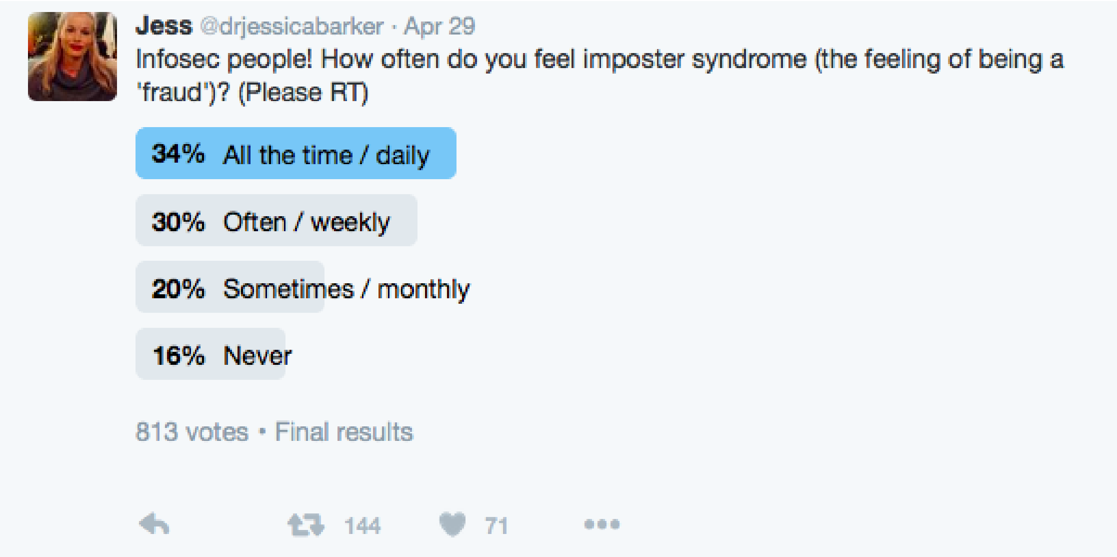
- As hiring mangers, we are implementing the policies set forth by the C-suite
- We are the front line to our defense

    Balancing the hard technical of our tools

    To the soft technical of human interactions

The Long Game

- Care and nurture of the team, of your staff
- Care and nurture of your community
- Impostor syndrome
- Managing up
- Potential discriminations
- Mental health/burnout



Jess @drjessicabarker · Apr 29

Infosec people! How often do you feel imposter syndrome (the feeling of being a 'fraud')? (Please RT)

34% All the time / daily

30% Often / weekly

20% Sometimes / monthly

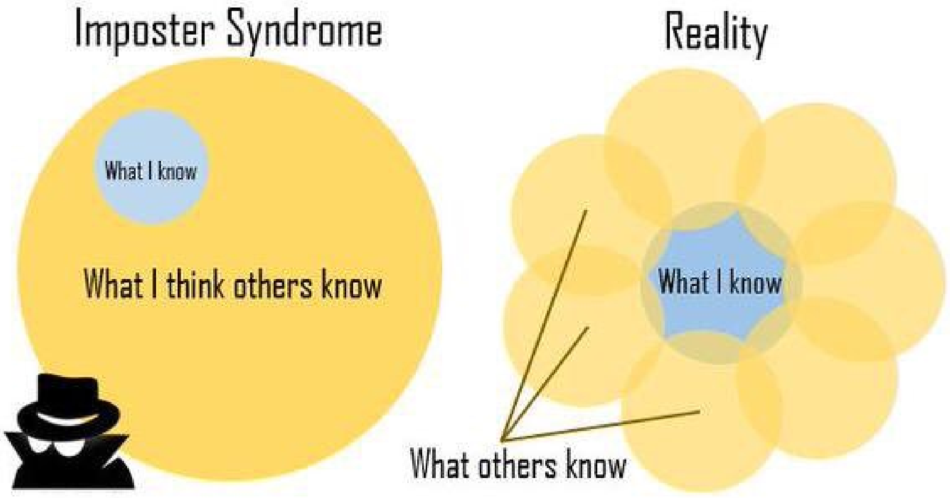
16% Never

813 votes • Final results

144 71

Impostor Syndrome

- Why occurrence of impostor syndrome in InfoSec?
  - Much ego in Infosec.
  - Infosec has purely attack/defense driven.
  - You are actively being attacked, often for money.
  - Nation states/Governments are now doing it in new and interesting ways, thus scarier.
  - InfoSec is becoming militarized
    - Sadly, “Cyber” is a thing
    - Guns and death & more ego.



Burnout

- Recognize analyst fatigue:
    - High false positive rate
    - Lack of attention to detail
        - Slower/less complete triage or containment activities
        - Incomplete incident or alert documentation
    - Calling count sick frequently/too much
    - Analysts not as “sharp” as in the past
    - High turnover
    - Little or no cross-training

Burnout Prevention

- Empower your team to not to have to churn through repetitive False Positives
- Embed senior analysts & engineers with your junior staff.
- Have regular day long “ride alongs” for those who have direct impact on analysts with their direct tasks.
- Have enough resources to allow for rotating project work; as well as dedicated training & StanEval.

    Each member should be learning something new and working on something that are not alerts regularly.

- Have a healthy reserve of alternate resources - either internal or external

Burnout Prevention

- Have a generous, enforced time-off policy.
- Have team building events.
- Crosstrain
- Rotate staff between roles
- Internal promotions
- Training and conferences
- Automate where possible
- Add data to provide context
- Nurture and build the “wolf team” aka hunters

The Long Term Impact

- When there is a mass exodus of security team members, word gets out there is something up in your environment
  - A previous event was the catalyst for everyone to start looking for a new opportunity
- Makes it even harder to attract & retain talent
- Be a leader, address issues early

  Your leadership directly relates to the team culture and hiring ability

Outside The Box

- Diversity
- Interns

  Long term pipeline, nurturing younger community
- Two year vs. four year schools

  Many two year schools have InfoSec programs
- Recruit and retain veterans

  Many Veterans have technical & InfoSec background
- Technical aptitude

  Help those communities teach

Long Term Fixes

- All said and done, how do we as hiring managers fix this?
- How do we change our paradigm on worthy candidates & hiring?

- How could/should applicants leverage our weakness to their favor?

Employers forget that the impression they leave on their employees, past & present, influences income, rep and biz dev in ways unknown.

@kjvalentine

References & Resources

Winn Schwartau, “Hiring the unhireable”

http://techspective.net/2015/07/06/hiring-the-unhireable-its-time-we-get-over-ourselves/

If Carpenters Were Hired Like Programmers

http://www.jasonbock.net/jb/News/Item/7c334037d1a9437d9fa6506e2f35eaac

Why 'True Recruiters' are actually Super Unicorns

https://www.linkedin.com/pulse/why-true-recruiters-actually-super-unicorns-ingeborg-van-harten

Evaluate the Scrapper

http://www.ted.com/talks/regina_hartley_why_the_best_hire_might_not_have_the_perfect_resume

Malory Isn’t the Only Imposter in Infosec

https://mumble.org.uk/blog/2016/04/30/malory-isnt-the-only-imposter-in-infosec/

Summary

- Set and adjust our expectations
- Our application processes are typically cumbersome and unwieldy, aim to improve them
- Our interviews may not provide the best opportunities for assessing capabilities and talent
- Our post-interview follow up is reflective of our communication styles and capabilities
- All areas for improvement

Take Aways

- Connect with at least 2 people post-meeting; learn how their application and selection process works (or not work).
- How can you be more active and involved in your local IT/InfoSec community?
- What can you do to mentor younger/less experienced?
- How can we improve our application process? Our screening process and criteria? Protect attacks via the application process?
- Have you ran a “pen test” on your application process?
- Review possible Social Engineering (SE) approaches, determine mitigations.

Criticisms & Rebuttal

But none of this is technical!!!1111

Social engineering is not technical? And then why do we keep messing it up?

This is stuff everyone knows!!!111 This is obvious!

Then why do we keep messing it up?

That was a lot of slides!

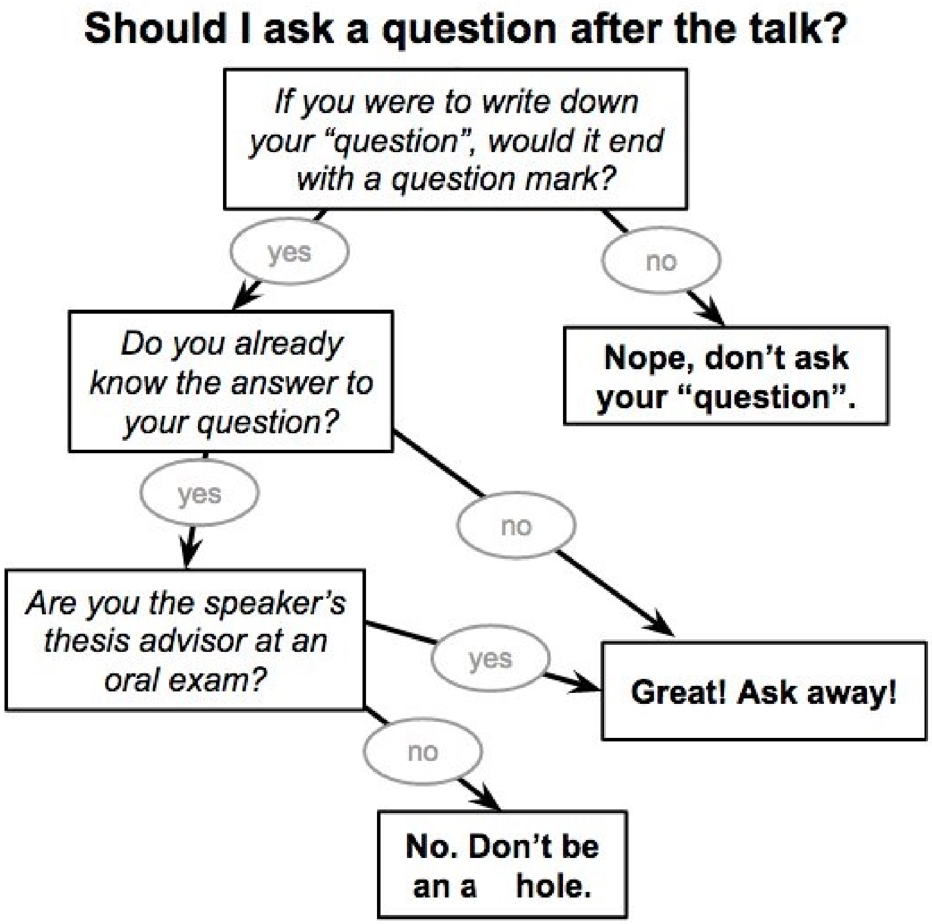
Yea, that is my presentation style.

Thanks (Credits)

@Tottenkoph
@StartUpJackson, @RebeccaSlatkin, @TylerSchmall, Trey Ford aka @treyford, @Jack_Daniel, Jackie Stokes aka @find_evil
roadtociso.wordpress.com - Jesika McEvoy
jasonbock.net - Jason Bock
@kjvalentine
John Omernik aka Chief Ten Beers
Winn Schwartau
mumble.org.uk - Ben Hughes

All those applications we submitted, those folks we interviewed with, and those we have interviewed.

Questions?
Thank you



Should I ask a question after the talk?

If you were to write down your "question", would it end with a question mark?

yes

no

Nope, don't ask your "question".

Do you already know the answer to your question?

yes

no

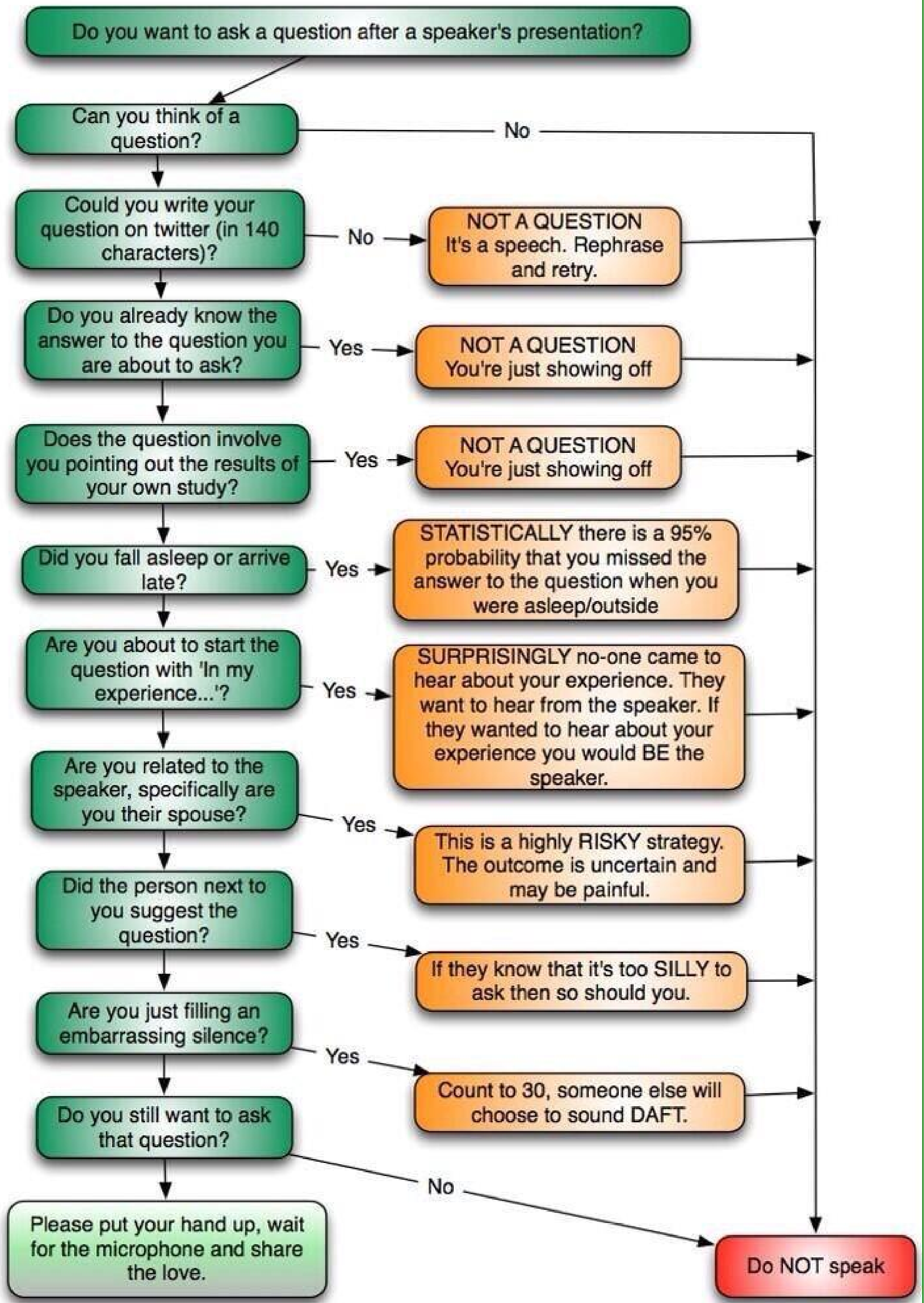
Are you the speaker's thesis advisor at an oral exam?

yes

Great! Ask away!

no

No. Don't be an a hole.



Do you want to ask a question after a speaker's presentation?

Can you think of a question?

No

Could you write your question on twitter (in 140 characters)?

No

NOT A QUESTION It's a speech. Rephrase and retry.

Do you already know the answer to the question you are about to ask?

Yes

NOT A QUESTION You're just showing off

Does the question involve you pointing out the results of your own study?

Yes

NOT A QUESTION You're just showing off

Did you fall asleep or arrive late?

Yes

STATISTICALLY there is a 95% probability that you missed the answer to the question when you were asleep/outside

Are you about to start the question with 'In my experience...'?

Yes

SURPRISINGLY no-one came to hear about your experience. They want to hear from the speaker. If they wanted to hear about your experience you would BE the speaker.

Are you related to the speaker, specifically are you their spouse?

Yes

This is a highly RISKY strategy. The outcome is uncertain and may be painful.

Did the person next to you suggest the question?

Yes

If they know that it's too SILLY to ask then so should you.

Are you just filling an embarrassing silence?

Yes

Count to 30, someone else will choose to sound DAFT.

Do you still want to ask that question?

No

Please put your hand up, wait for the microphone and share the love.

Do NOT speak