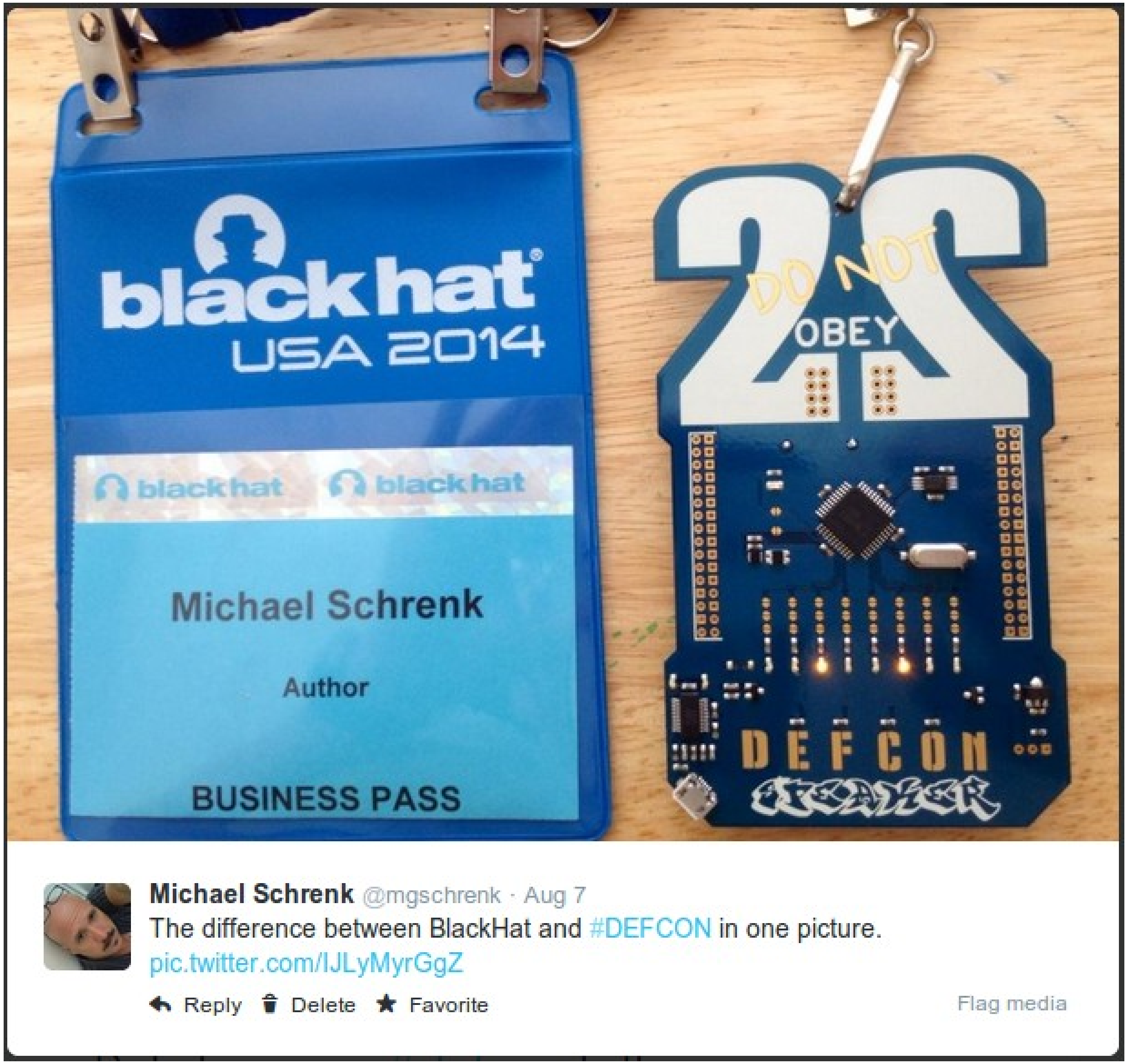
DEFCON 22

You're Leaking TRADE SECRETS

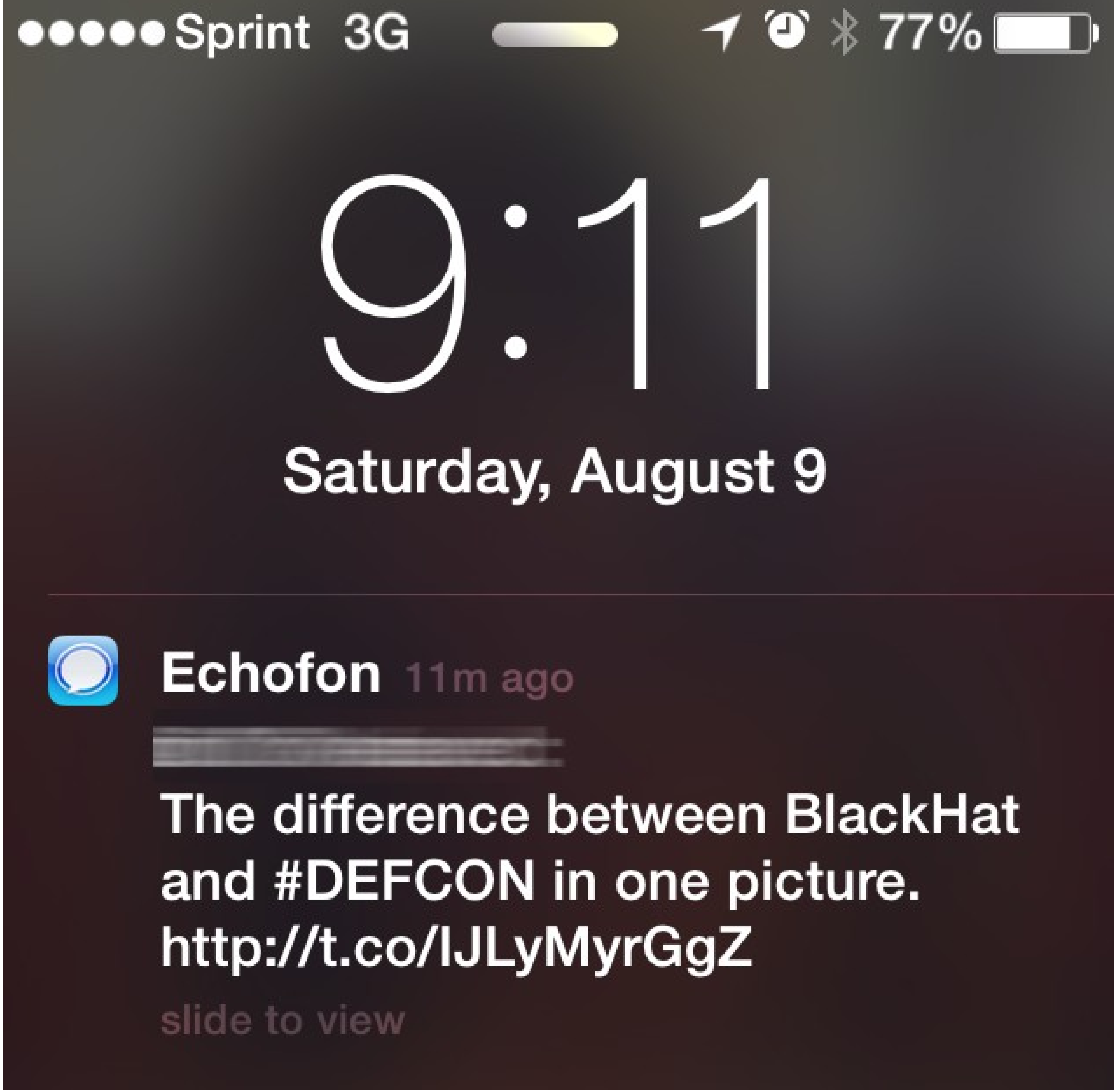
You're Leaking Trade Secrets

You're Leaking Trade Secrets



Michael Schrenk @mgschrenk · Aug 7
The difference between BlackHat and #DEFCON in one picture.
pic.twitter.com/lJLyMyrGgZ

You're Leaking Trade Secrets



9:11

Saturday, August 9

Echofon 11m ago

[redacted]

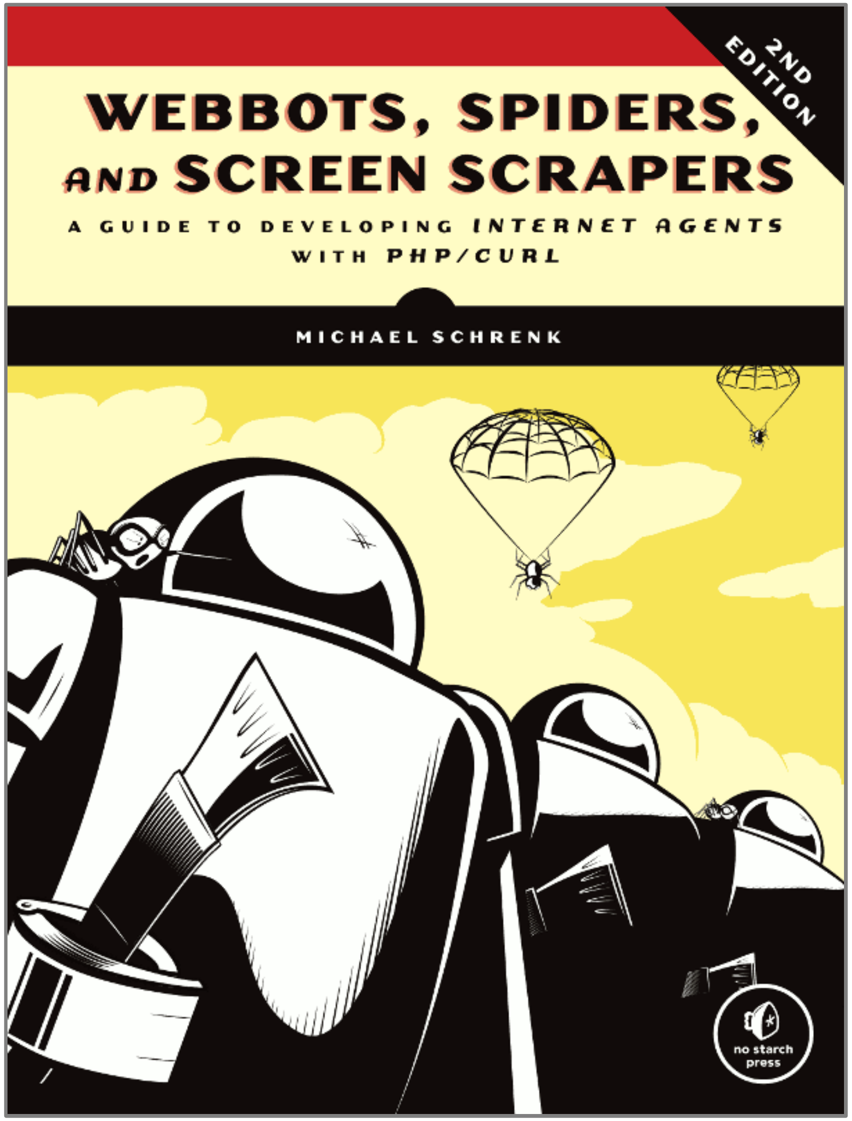
The difference between BlackHat and #DEFCON in one picture. http://t.co/lJLyMyrGgZ

slide to view

Michael Schrenk

twitter:
@mgschrenk

facebook:
facebook.com/webbots


2ND EDITION
WEBBOTS, SPIDERS, AND SCREEN SCRAPERS
A GUIDE TO DEVELOPING INTERNET AGENTS WITH PHP/CURL
MICHAEL SCHRENK
no starch press

This is a story about

Organizational
Privacy

Individuals unintentionally leak **identity**

You're Leaking Trade Secrets

Individuals unintentionally leak **identity**

Organizations unintentionally leak **trade secrets**

Spoiler Alert:

Not all online information is:

- Read by the intended audience

Spoiler Alert:

Not all online information is:

- Read by the intended audience
- Used as intended

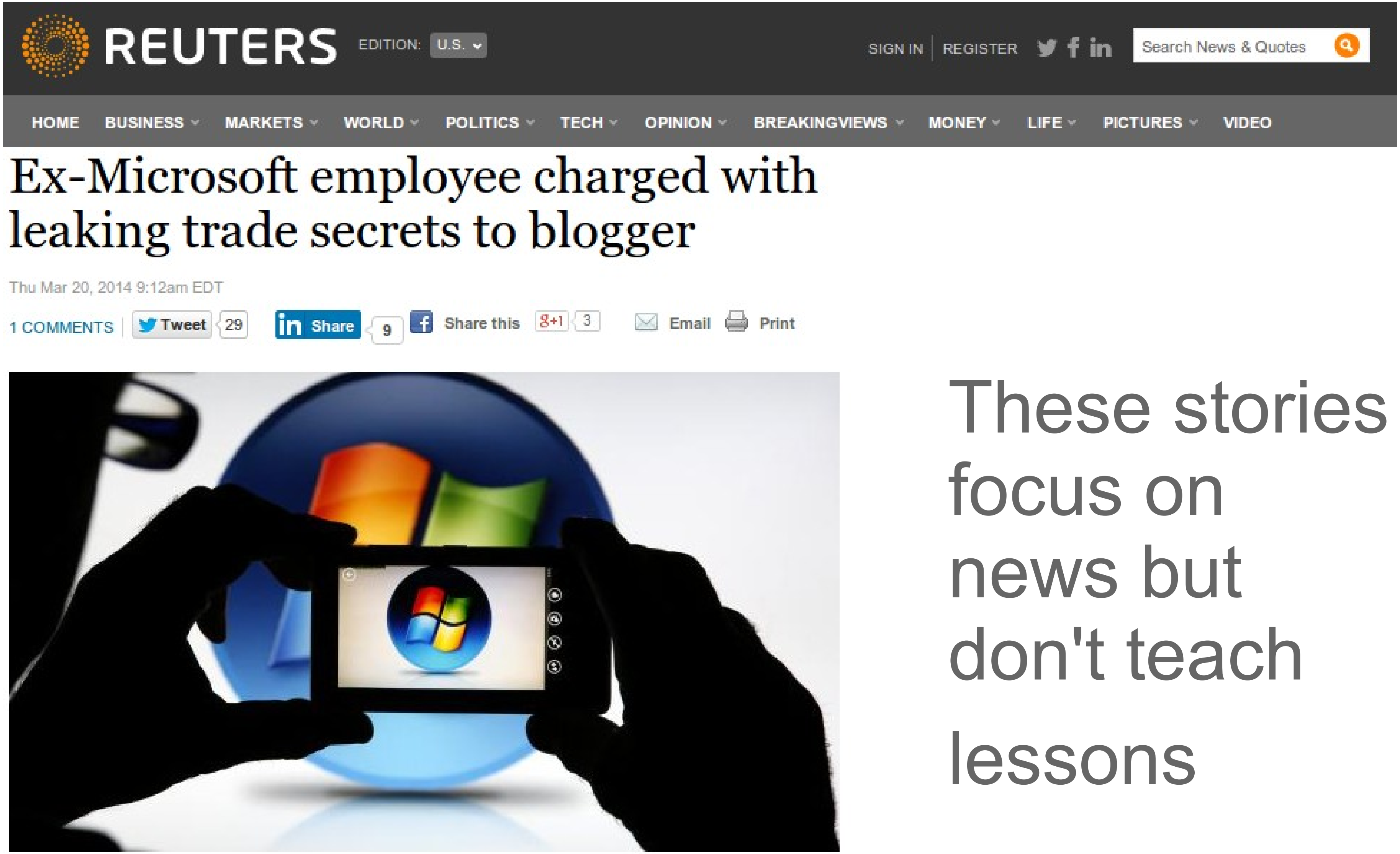
Individuals are aware of the need for **personal** privacy

Individuals are aware of the need for **personal** privacy

Organizations are less aware of the need for **organizational** privacy

The difference in awareness is largely due to the media, and how they cover privacy stories

Articles on Trade Secrets only focus on crimes



Ex-Microsoft employee charged with leaking trade secrets to blogger

Thu Mar 20, 2014 9:12am EDT

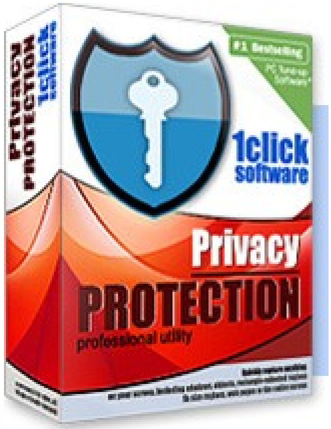
These stories focus on news but don't teach lessons

You're Leaking Trade Secrets

Personal privacy stories create many customers for a host of advertisers

LifeLock.
#1 In Identity Theft Protection®

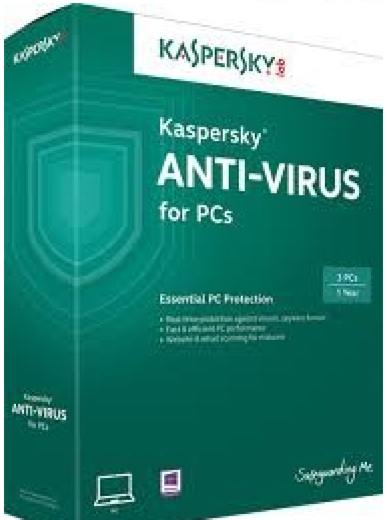
IdentityForce.™



symantec.™

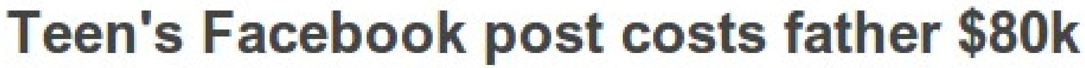
Norton™
by Symantec

IDENTITY GUARD.
www.IdentityGuard.com



McAfee®
Proven Security™

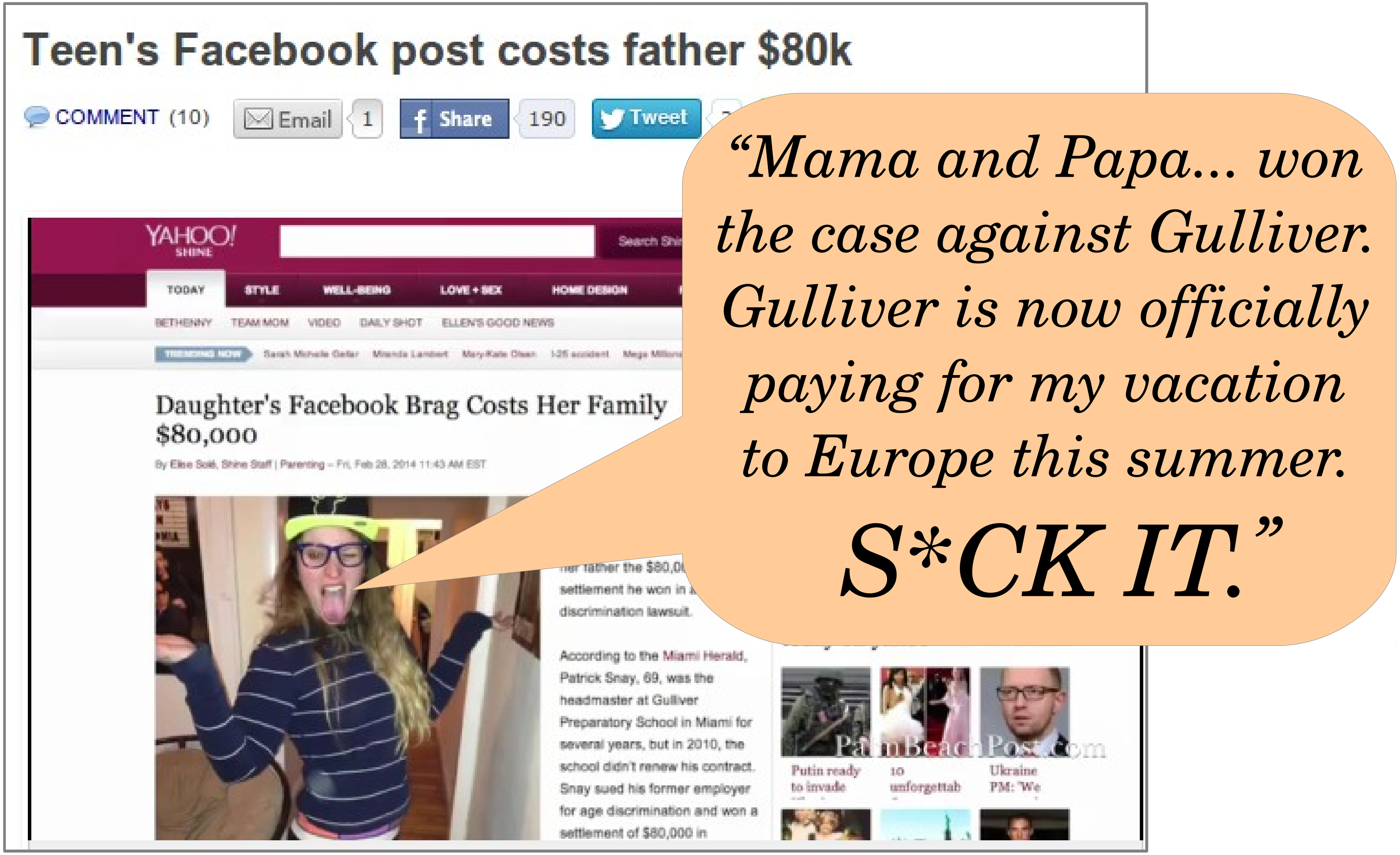
Personal privacy stories create great content



Teen's Facebook post costs father $80k

You're Leaking Trade Secrets

Personal privacy stories create great content



Teen's Facebook post costs father $80k

Daughter's Facebook Brag Costs Her Family $80,000

By Elise Solé, Shine Staff | Parenting – Fri, Feb 28, 2014 11:43 AM EST

her father the $80,0 settlement he won in a discrimination lawsuit.

According to the Miami Herald, Patrick Snay, 69, was the headmaster at Gulliver Preparatory School in Miami for several years, but in 2010, the school didn't renew his contract. Snay sued his former employer for age discrimination and won a settlement of $80,000 in

PalmBeachPost.com
Putin ready to invade
10 unforgettab
Ukraine PM: 'We
"Mama and Papa... won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. S*CK IT."

Personal privacy stories create great content

Selfie geotags reveal location of soldier

Personal privacy stories create great content

Selfie geotags reveal location of soldier

These stories teach Important lessons

In this talk...

- Define “trade secrets”
- Examples: **unintentional** leaks
- Online business intelligence
- What can be done to minimize **unintentional** leaks

In this talk...

- Define “trade secrets”
- Examples: **unintentional** leaks
- Online business intelligence
- What can be done to minimize **unintentional** leaks

In this talk...

- Define “trade secrets”
- Examples: **unintentional** leaks
- Online business intelligence
- What can be done to minimize **unintentional** leaks

In this talk...

- Define “trade secrets”
- Examples: **unintentional** leaks
- Online business intelligence
- What can be done to minimize **unintentional** leaks

What is a Trade Secret?

- Don't need to be published
- Have no expiration dates
- Protected by the UTSA (Uniform Trade Secrets Act)

What is a Trade Secret?

- Don't need to be published
- Have no expiration dates
- Protected by the UTSA (Uniform Trade Secrets Act)

What is a Trade Secret?

- Don't need to be published
- Have no expiration dates
- Protected by the UTSA (Uniform Trade Secrets Act)

What is a Trade Secret?

- Don't need to be published
- Have no expiration dates
- Protected by the UTSA (Uniform Trade Secrets Act)

Trade Secrets are “special” intellectual property

- Must have economic value
- Anyone can use another's trade secret if discovered

Trade Secrets are “special” intellectual property

- Must have economic value
- Anyone can use another's trade secret if discovered

What is the value of a Trade Secret?

Once a trade secret is established, the owner may prevent other parties from misappropriating the trade secret

Trade Secrets Examples
Recipes & Formulas

The recipe for Coca-Cola

The formula for Chanel No. 5

You're Leaking Trade Secrets

Trade Secrets Examples
Processes

Patents describe GM's inventions, but the implementation of those ideas are trade secrets

Data as Trade Secrets

Employee lists, Supplier contacts, Customer lists, Funding sources, Expansion plans, Marketing plans, New product planning, Pricing strategies, Supplier issues, Labor issues, Sales rates, Inventory turnover rates, Slow merchandise, Fast merchandise, IT infrastructure changes, Security information,

You're Leaking Trade Secrets

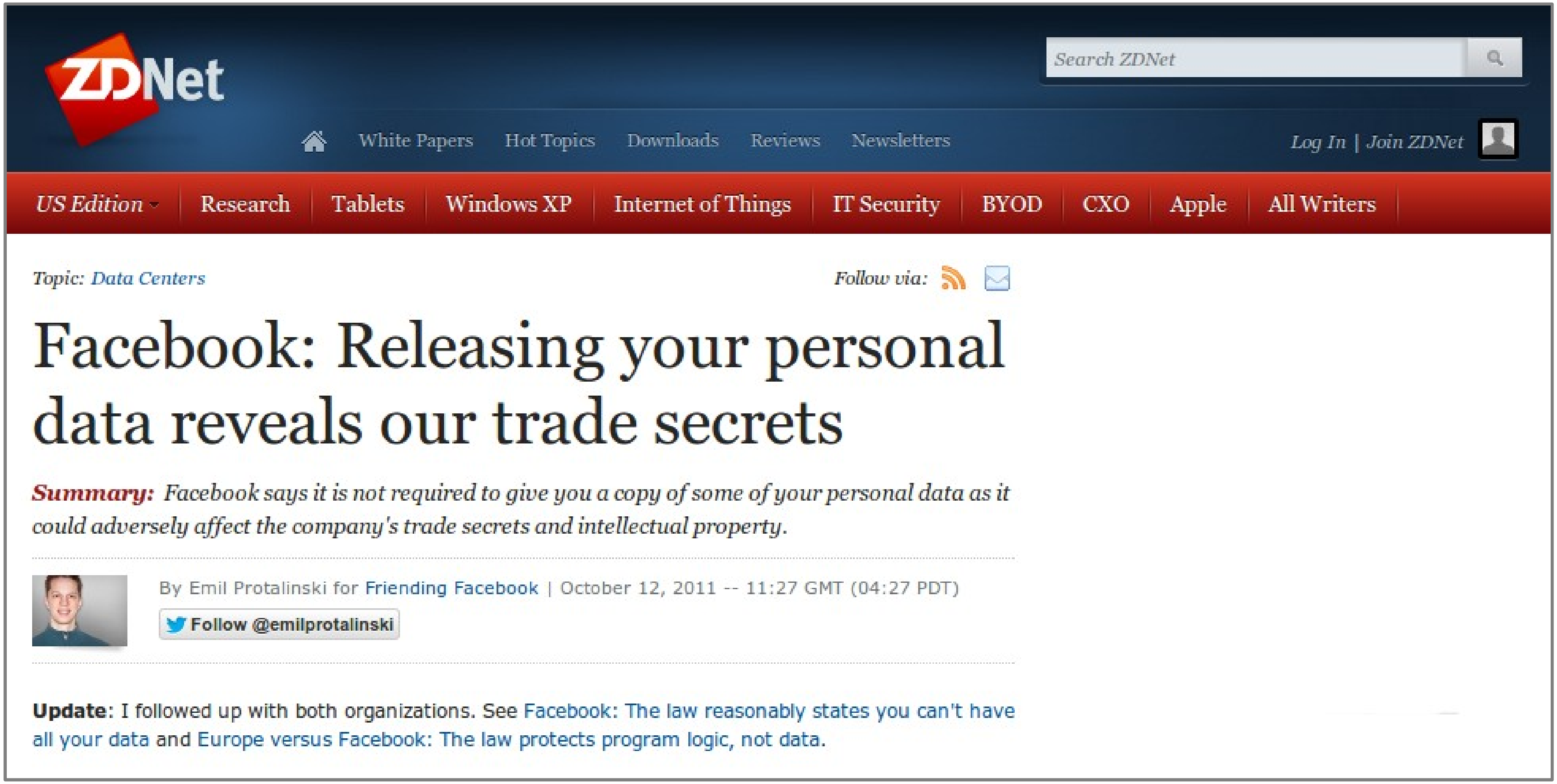
Data as Trade Secrets

Employee lists, Supplier contacts, Customer lists, Funding sources, Expansion plans, Marketing plans, New product planning, Pricing strategies, Supplier issues, Labor issues, Sales rates, Inventory turnover rates, Slow merchandise, Fast merchandise, IT infrastructure changes, Security information,

This list unique for every industry

Data as Trade Secrets

Facebook responds to European Union privacy laws



Topic: Data Centers

Facebook: Releasing your personal data reveals our trade secrets

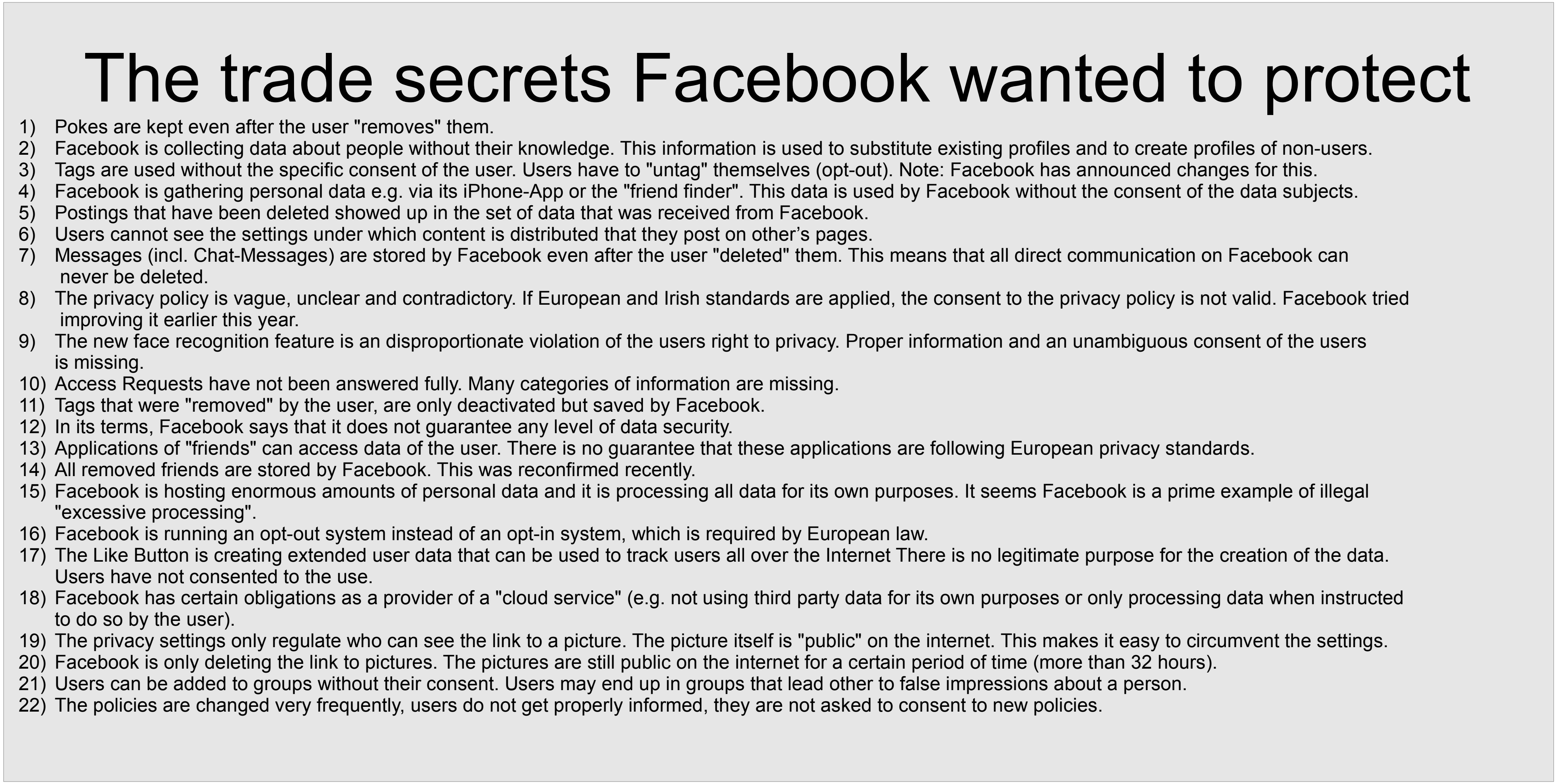
Summary: *Facebook says it is not required to give you a copy of some of your personal data as it could adversely affect the company's trade secrets and intellectual property.*

By Emil Protalinski for Friending Facebook | October 12, 2011 -- 11:27 GMT (04:27 PDT)

Update: I followed up with both organizations. See Facebook: The law reasonably states you can't have all your data and Europe versus Facebook: The law protects program logic, not data.

Data as Trade Secrets

Facebook responds to European Union privacy laws



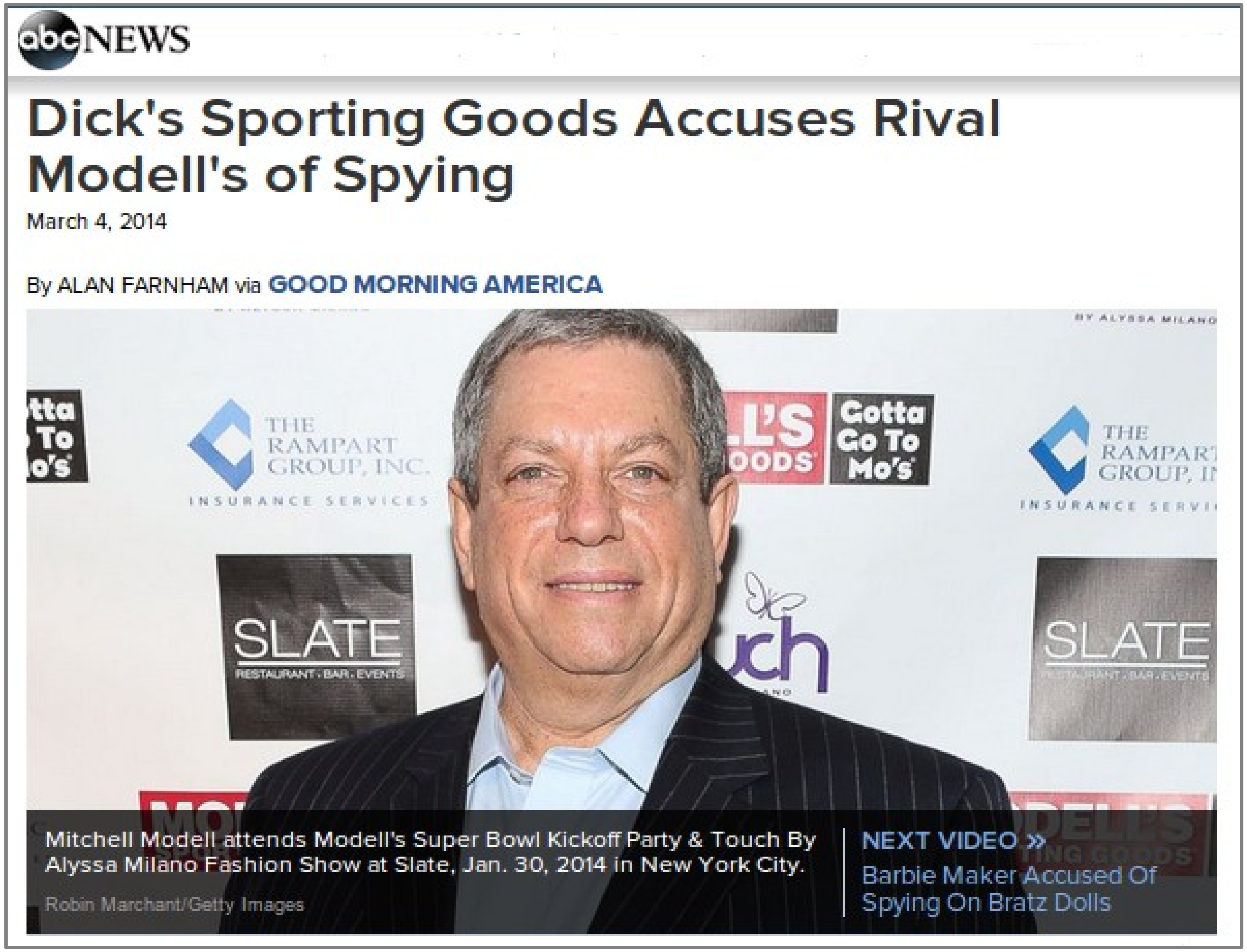
The trade secrets Facebook wanted to protect

1) Pokes are kept even after the user "removes" them.
2) Facebook is collecting data about people without their knowledge. This information is used to substitute existing profiles and to create profiles of non-users.
3) Tags are used without the specific consent of the user. Users have to "untag" themselves (opt-out). Note: Facebook has announced changes for this.
4) Facebook is gathering personal data e.g. via its iPhone-App or the "friend finder". This data is used by Facebook without the consent of the data subjects.
5) Postings that have been deleted showed up in the set of data that was received from Facebook.
6) Users cannot see the settings under which content is distributed that they post on other's pages.
7) Messages (incl. Chat-Messages) are stored by Facebook even after the user "deleted" them. This means that all direct communication on Facebook can never be deleted.
8) The privacy policy is vague, unclear and contradictory. If European and Irish standards are applied, the consent to the privacy policy is not valid. Facebook tried improving it earlier this year.
9) The new face recognition feature is an disproportionate violation of the users right to privacy. Proper information and an unambiguous consent of the users is missing.
10) Access Requests have not been answered fully. Many categories of information are missing.
11) Tags that were "removed" by the user, are only deactivated but saved by Facebook.
12) In its terms, Facebook says that it does not guarantee any level of data security.
13) Applications of "friends" can access data of the user. There is no guarantee that these applications are following European privacy standards.
14) All removed friends are stored by Facebook. This was reconfirmed recently.
15) Facebook is hosting enormous amounts of personal data and it is processing all data for its own purposes. It seems Facebook is a prime example of illegal "excessive processing".
16) Facebook is running an opt-out system instead of an opt-in system, which is required by European law.
17) The Like Button is creating extended user data that can be used to track users all over the Internet There is no legitimate purpose for the creation of the data. Users have not consented to the use.
18) Facebook has certain obligations as a provider of a "cloud service" (e.g. not using third party data for its own purposes or only processing data when instructed to do so by the user).
19) The privacy settings only regulate who can see the link to a picture. The picture itself is "public" on the internet. This makes it easy to circumvent the settings.
20) Facebook is only deleting the link to pictures. The pictures are still public on the internet for a certain period of time (more than 32 hours).
21) Users can be added to groups without their consent. Users may end up in groups that lead other to false impressions about a person.
22) The policies are changed very frequently, users do not get properly informed, they are not asked to consent to new policies.

You're Leaking Trade Secrets

The Internet has changed how Business Intelligence is collected

Prior to 1995, trade secrets were discovered like this



abcNEWS

Dick's Sporting Goods Accuses Rival Modell's of Spying

March 4, 2014

By ALAN FARNHAM via GOOD MORNING AMERICA

Mitchell Modell attends Modell's Super Bowl Kickoff Party & Touch By Alyssa Milano Fashion Show at Slate, Jan. 30, 2014 in New York City.

Robin Marchant/Getty Images

NEXT VIDEO »

Barbie Maker Accused Of Spying On Bratz Dolls

Prior to 1995, trade secrets were discovered like this

Mitch Modell, on the television show, Undercover Boss

You're Leaking Trade Secrets

The Internet has changed Business Intelligence

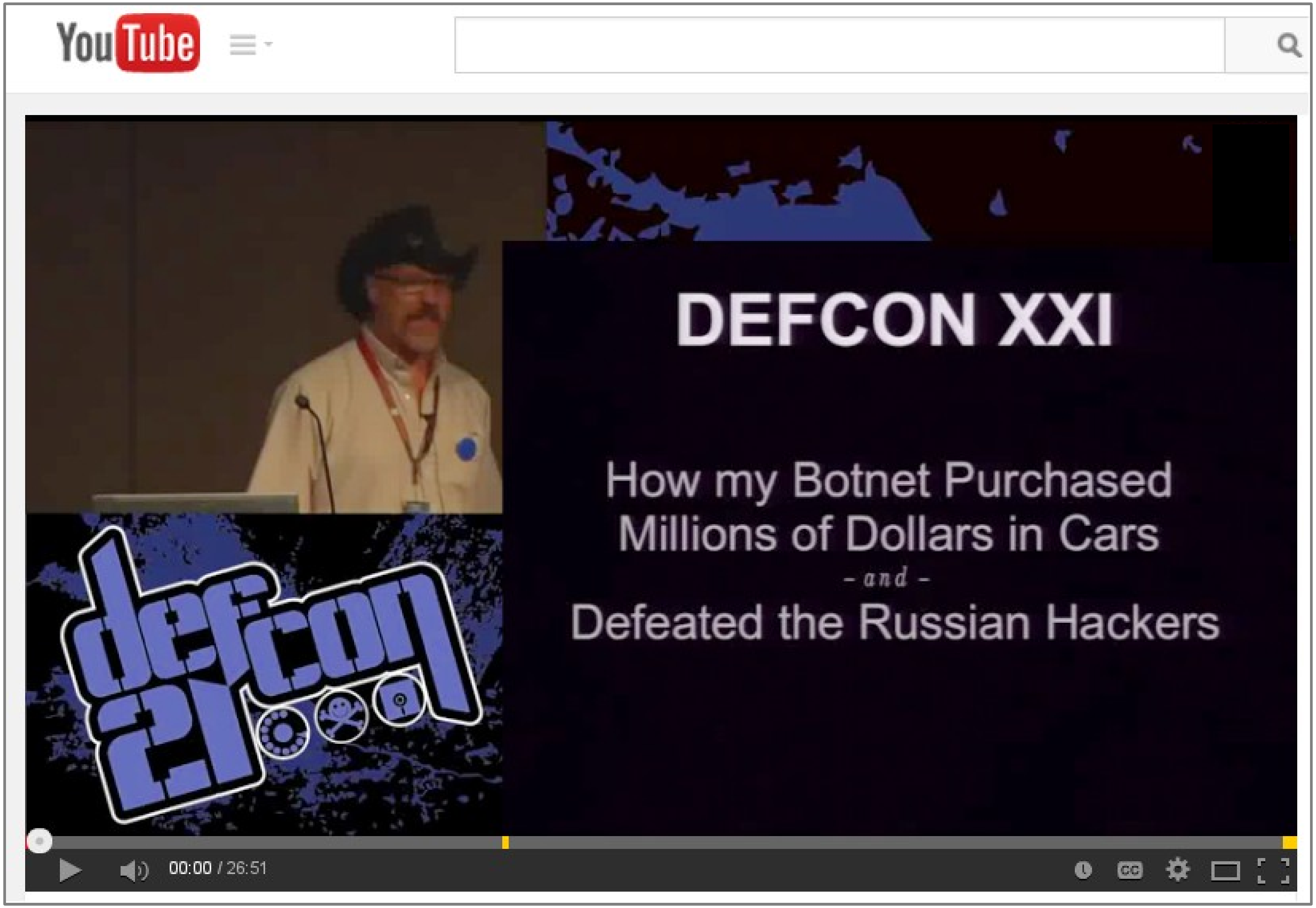
Before 1995	After 1995
There were a limited number of sources	The number of Business Intelligence sources is unlimited
BI was a time consuming, manual, & expensive process	Automated collection, repeated – trends can be analyzed in real-time
It required physical contact	Can be done remotely
Often required researchers to identify themselves	Can (usually) be done anonymously

The Internet has changed Business Intelligence

Before 1995	After 1995
There were a limited number of sources	The number of Business Intelligence sources is unlimited
BI was a time consuming, manual, & expensive process	Automated collection, repeated – trends can be analyzed in real-time
It required physical contact	Can be done remotely
Often required researchers to identify themselves	Can (usually) be done anonymously

You're Leaking Trade Secrets

Secrets found online are immediately actionable



DEFCON XXI

How my Botnet Purchased Millions of Dollars in Cars

- and -

Defeated the Russian Hackers

The Internet has changed Business Intelligence

Through the eyes of a hacker, anything you put online is potential Business Intelligence.

Web page updates create databases of information

Every industry has it's own cases.

Here are a few that anyone
from any industry can relate.

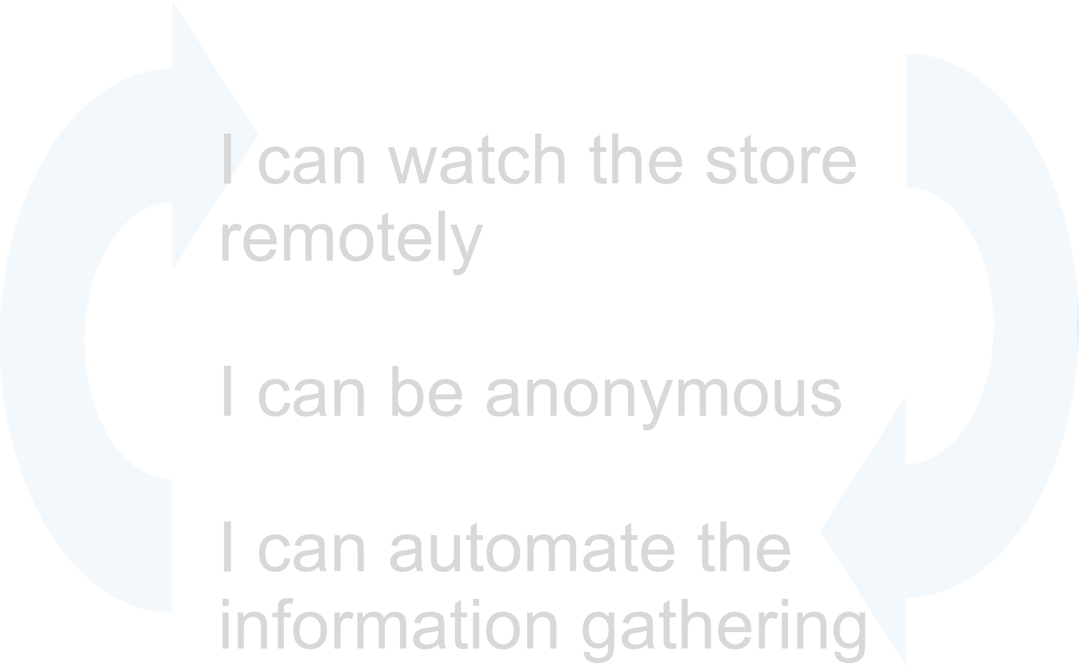
Monitored retail websites leak trade secrets

What online retailer thinks

I need to keep my online store up to Date.

I need to keep up with competitor pricing changes.

What a hacker thinks



I can watch the store remotely

I can be anonymous

I can automate the information gathering

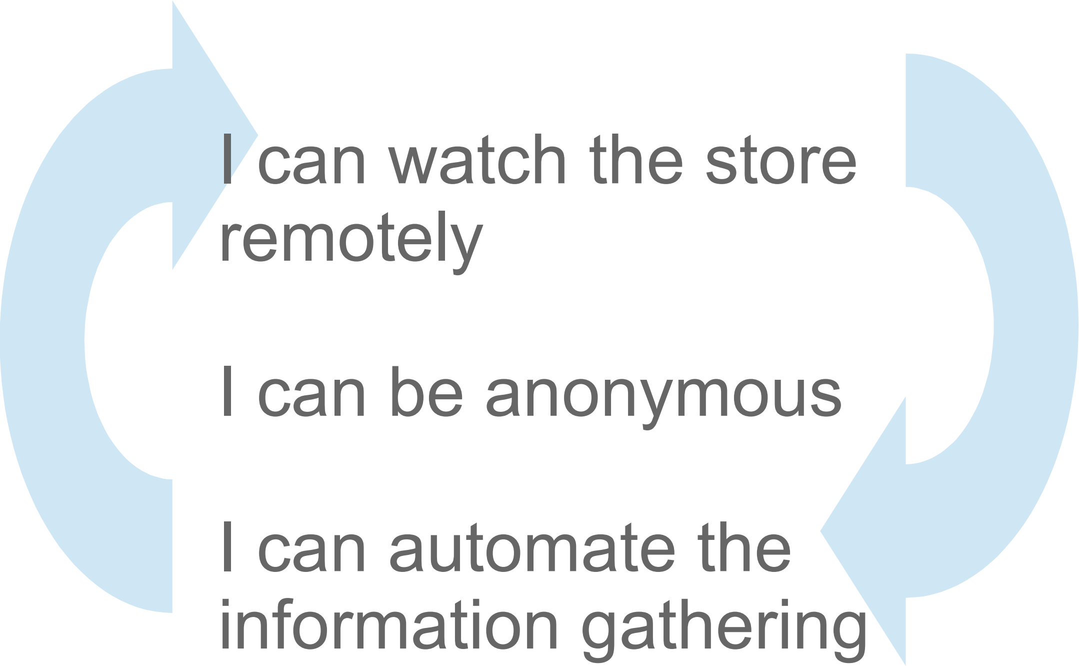
Monitored retail websites leak trade secrets

What online retailer thinks

I need to keep my Online store up to Date.

I need to keep up with competitor pricing changes.

What a hacker thinks



I can watch the store remotely

I can be anonymous

I can automate the information gathering

You're Leaking Trade Secrets

Monitored retail websites leak trade secrets

A monitored retail site, monitored over time, can leak...

- Pricing strategies
- Inventory strategies
- Supplier issues
- Supplier sources

Monitored retail websites leak trade secrets

The problem of leaking trade secrets is much worse for retailers that sell specific items.

- Real estate websites
- Esty crafters
- eBay merchants
- Used book stores
- 3rd party Amazon retailers
- Car dealerships
- Sellers of collectibles

Monitored retail websites leak trade secrets

The problem of leaking trade secrets is much worse for retailers that sell specific items.

- Car dealerships
- Esty crafters
- eBay merchants
- Used book stores
- 3rd party Amazon retailers
- Sellers of collectibles
- Real estate websites

This group includes everyone selling uniquely identifiable goods

Monitored retail websites leak trade secrets

Businesses that sell specific items online, disclose their entire sales records

When you monitor this information over a period of time...

Monitored retail websites leak trade secrets

Businesses that sell specific items online, disclose their entire sales records

When you monitor this information over a period of time...

You essentially have enough information to do their accounting

You're Leaking Trade Secrets

Monitored job postings leak strategic planning

What HR thinks

I'm going to post 250
Job postings this year

What a hacker thinks

I can watch job postings remotely

I can be anonymous

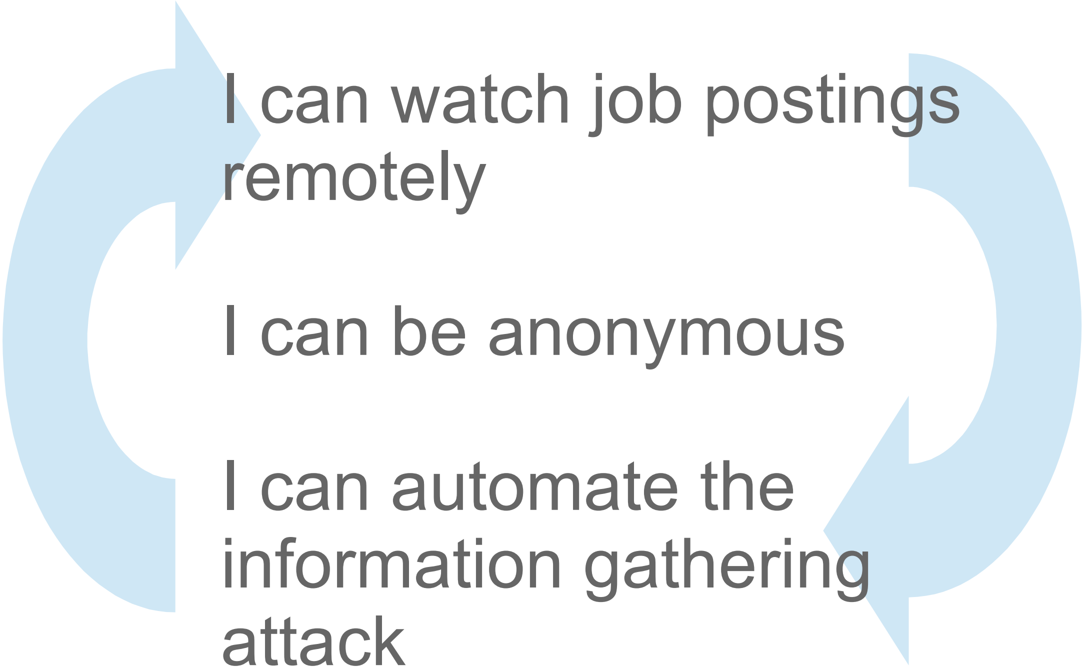
I can automate the information gathering attack

Monitored job postings leak strategic planning

What HR thinks

I'm going to post 250
Job postings this year

What a hacker thinks



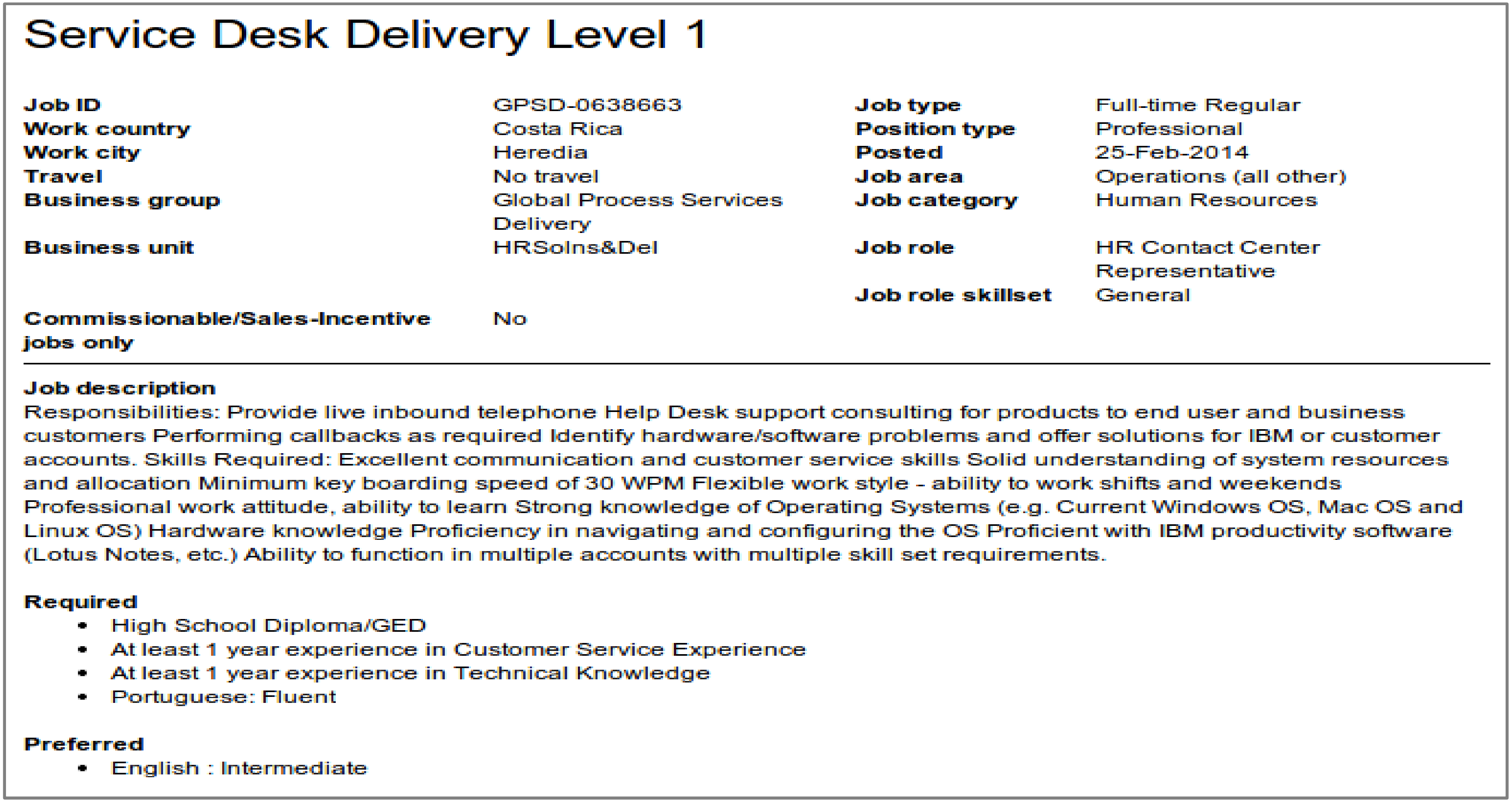
I can watch job postings remotely

I can be anonymous

I can automate the information gathering attack

Monitored job postings leak strategic planning

Even good job postings can be problematic



Service Desk Delivery Level 1

Job ID	GPSD-0638663	**Job type**	Full-time Regular
Work country	Costa Rica	**Position type**	Professional
Work city	Heredia	**Posted**	25-Feb-2014
Travel	No travel	**Job area**	Operations (all other)
Business group	Global Process Services Delivery	**Job category**	Human Resources
Business unit	HRSolns&Del	**Job role**	HR Contact Center Representative
		Job role skillset	General
Commissionable/Sales-Incentive jobs only	No		

Job description

Responsibilities: Provide live inbound telephone Help Desk support consulting for products to end user and business customers Performing callbacks as required Identify hardware/software problems and offer solutions for IBM or customer accounts. Skills Required: Excellent communication and customer service skills Solid understanding of system resources and allocation Minimum key boarding speed of 30 WPM Flexible work style - ability to work shifts and weekends Professional work attitude, ability to learn Strong knowledge of Operating Systems (e.g. Current Windows OS, Mac OS and Linux OS) Hardware knowledge Proficiency in navigating and configuring the OS Proficient with IBM productivity software (Lotus Notes, etc.) Ability to function in multiple accounts with multiple skill set requirements.

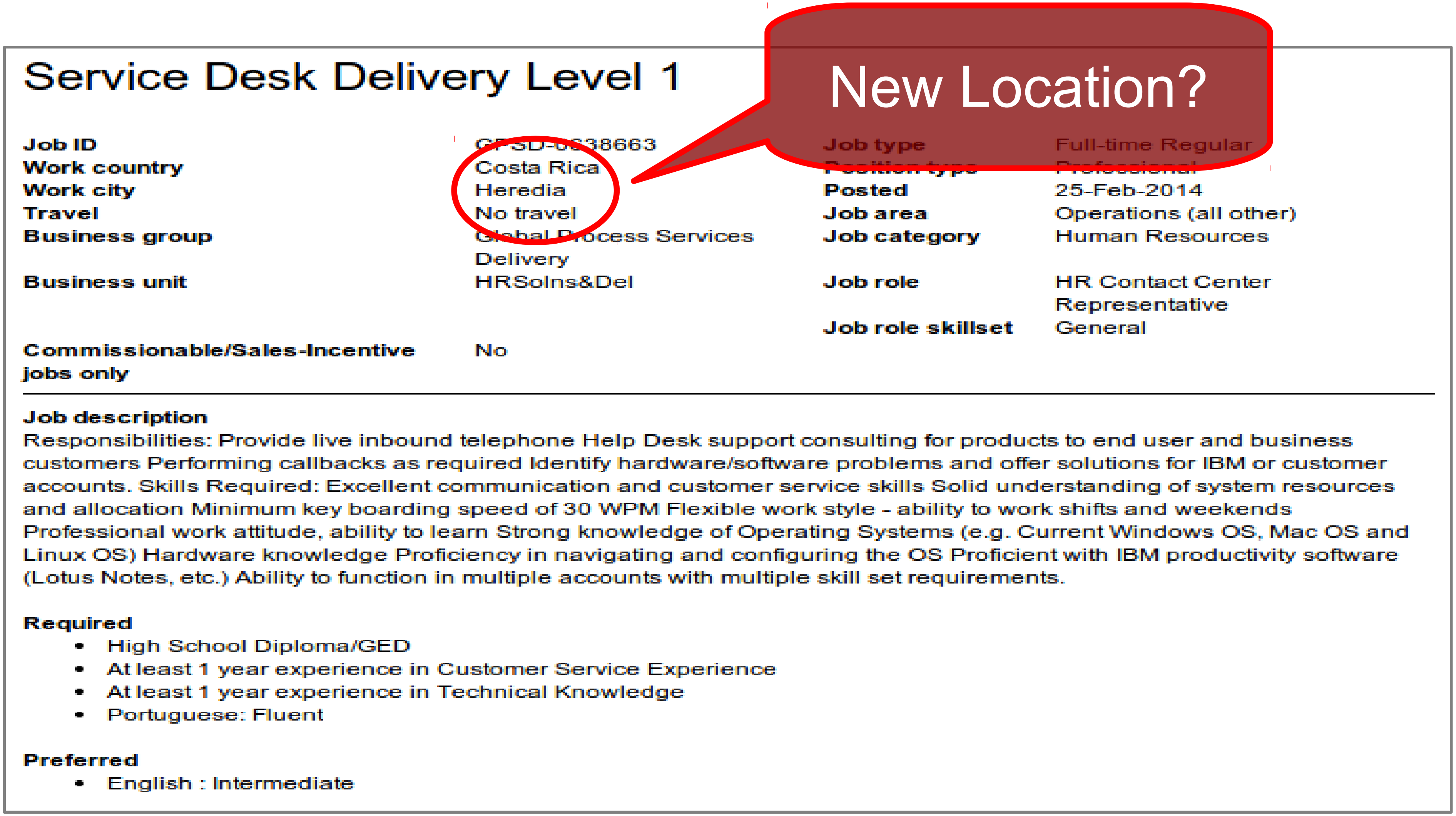
Required

- High School Diploma/GED
- At least 1 year experience in Customer Service Experience
- At least 1 year experience in Technical Knowledge
- Portuguese: Fluent

Preferred

- English : Intermediate

Monitored job postings leak strategic planning



New Location?

Service Desk Delivery Level 1

Job ID	GPSD-0638663	**Job type**	Full-time Regular
Work country	Costa Rica	**Position type**	Professional
Work city	Heredia	**Posted**	25-Feb-2014
Travel	No travel	**Job area**	Operations (all other)
Business group	Global Process Services Delivery	**Job category**	Human Resources
Business unit	HRSolns&Del	**Job role**	HR Contact Center Representative
		Job role skillset	General
Commissionable/Sales-Incentive jobs only	No		

Job description
Responsibilities: Provide live inbound telephone Help Desk support consulting for products to end user and business customers Performing callbacks as required Identify hardware/software problems and offer solutions for IBM or customer accounts. Skills Required: Excellent communication and customer service skills Solid understanding of system resources and allocation Minimum key boarding speed of 30 WPM Flexible work style - ability to work shifts and weekends Professional work attitude, ability to learn Strong knowledge of Operating Systems (e.g. Current Windows OS, Mac OS and Linux OS) Hardware knowledge Proficiency in navigating and configuring the OS Proficient with IBM productivity software (Lotus Notes, etc.) Ability to function in multiple accounts with multiple skill set requirements.

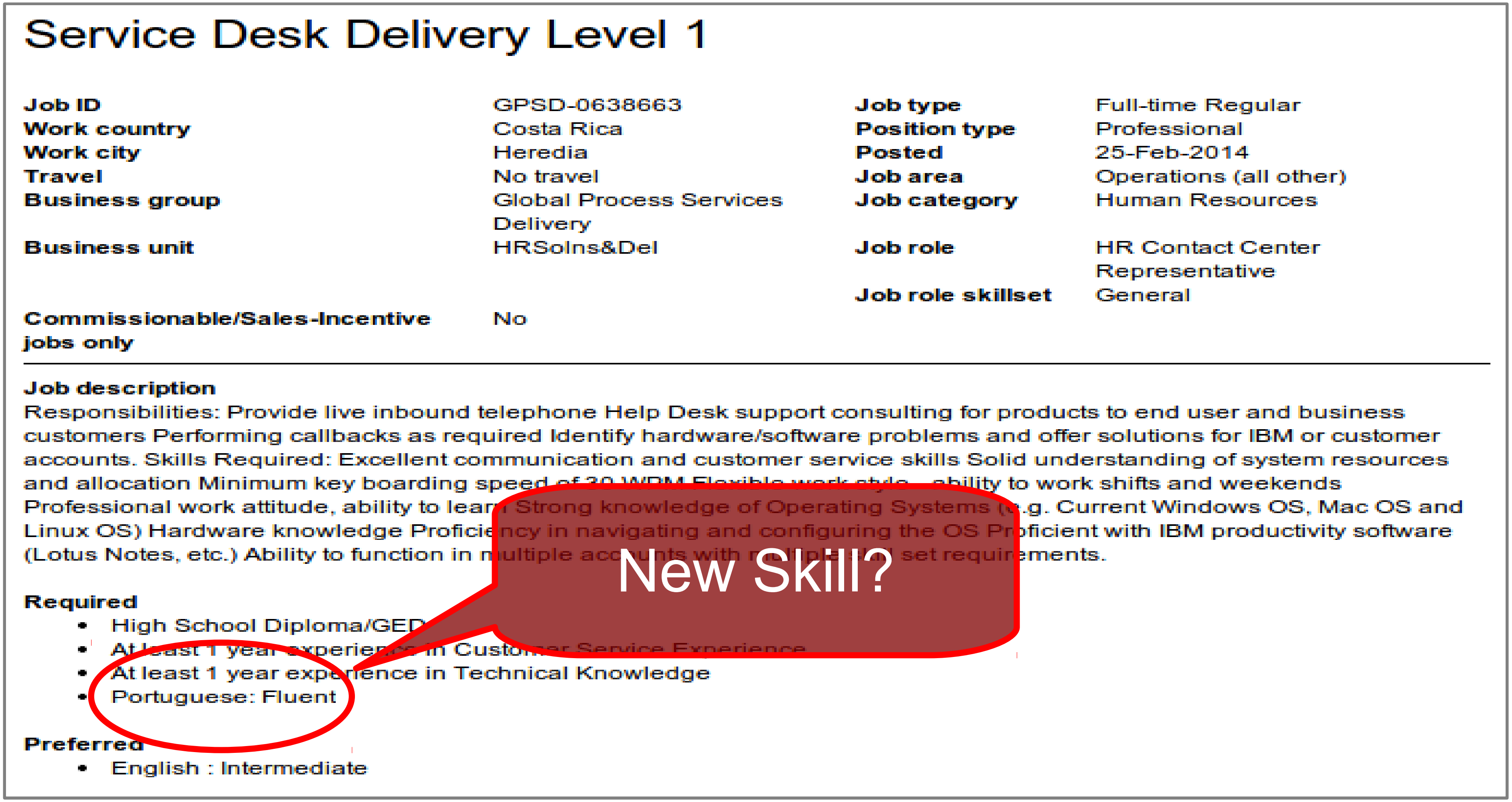
Required

- High School Diploma/GED
- At least 1 year experience in Customer Service Experience
- At least 1 year experience in Technical Knowledge
- Portuguese: Fluent

Preferred

- English : Intermediate

Monitored job postings leak strategic planning



Service Desk Delivery Level 1

Job ID	GPSD-0638663	**Job type**	Full-time Regular
Work country	Costa Rica	**Position type**	Professional
Work city	Heredia	**Posted**	25-Feb-2014
Travel	No travel	**Job area**	Operations (all other)
Business group	Global Process Services Delivery	**Job category**	Human Resources
Business unit	HRSolns&Del	**Job role**	HR Contact Center Representative
		Job role skillset	General
Commissionable/Sales-Incentive jobs only	No		

Job description
Responsibilities: Provide live inbound telephone Help Desk support consulting for products to end user and business customers Performing callbacks as required Identify hardware/software problems and offer solutions for IBM or customer accounts. Skills Required: Excellent communication and customer service skills Solid understanding of system resources and allocation Minimum key boarding speed of 30 WPM Flexible work style , ability to work shifts and weekends Professional work attitude, ability to learn Strong knowledge of Operating Systems (e.g. Current Windows OS, Mac OS and Linux OS) Hardware knowledge Proficiency in navigating and configuring the OS Proficient with IBM productivity software (Lotus Notes, etc.) Ability to function in multiple accounts with multiple skill set requirements.

Required

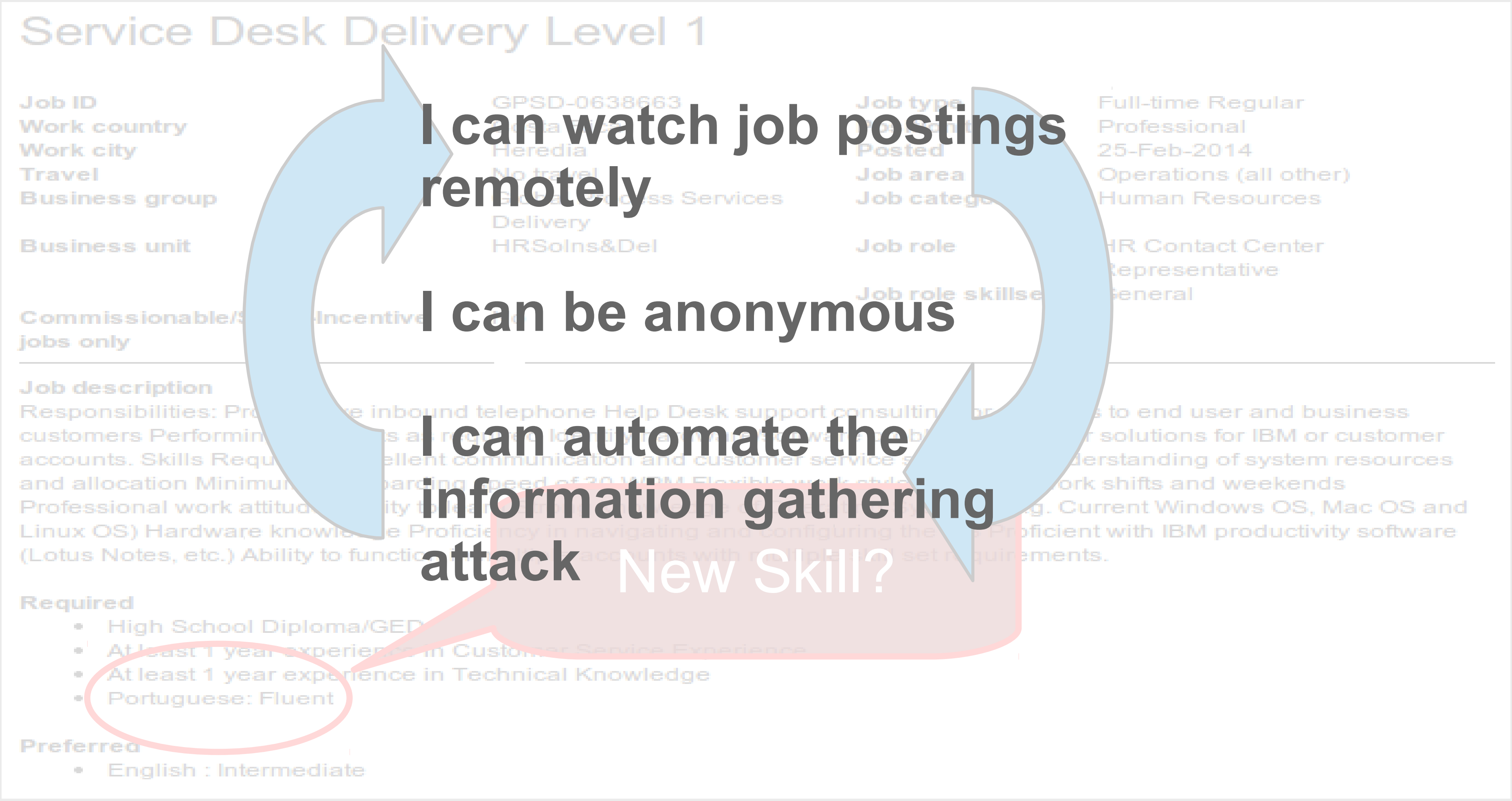
- High School Diploma/GED
- At least 1 year experience in Customer Service Experience
- At least 1 year experience in Technical Knowledge
- Portuguese: Fluent

Preferred

- English : Intermediate

New Skill?

Monitored job postings leak strategic planning



I can watch job postings remotely

I can be anonymous

I can automate the information gathering attack

Service Desk Delivery Level 1

Job ID	GPSD-0638663	Job type	Full-time Regular
Work country	[illegible]	[illegible]	Professional
Work city	Heredia	Posted	25-Feb-2014
Travel	No travel	Job area	Operations (all other)
Business group	[illegible] ss Services Delivery	Job catego[illegible]	Human Resources
Business unit	HRSolns&Del	Job role	HR Contact Center Representative
		Job role skillse[illegible]	General
Commissionable/S[illegible] Incentive jobs only	[illegible]		

Job description

Responsibilities: Pro[illegible] inbound telephone Help Desk support consultin[illegible] to end user and business customers Performin[illegible] s as re[illegible] r solutions for IBM or customer accounts. Skills Requ[illegible] ellent communication and customer service s[illegible] derstanding of system resources and allocation Minimu[illegible] ork shifts and weekends Professional work attitu[illegible] g. Current Windows OS, Mac OS and Linux OS) Hardware knowle[illegible] e Proficiency in navigating and configuring the [illegible] Proficient with IBM productivity software (Lotus Notes, etc.) Ability to functio[illegible] set r[illegible] quirements.

Required

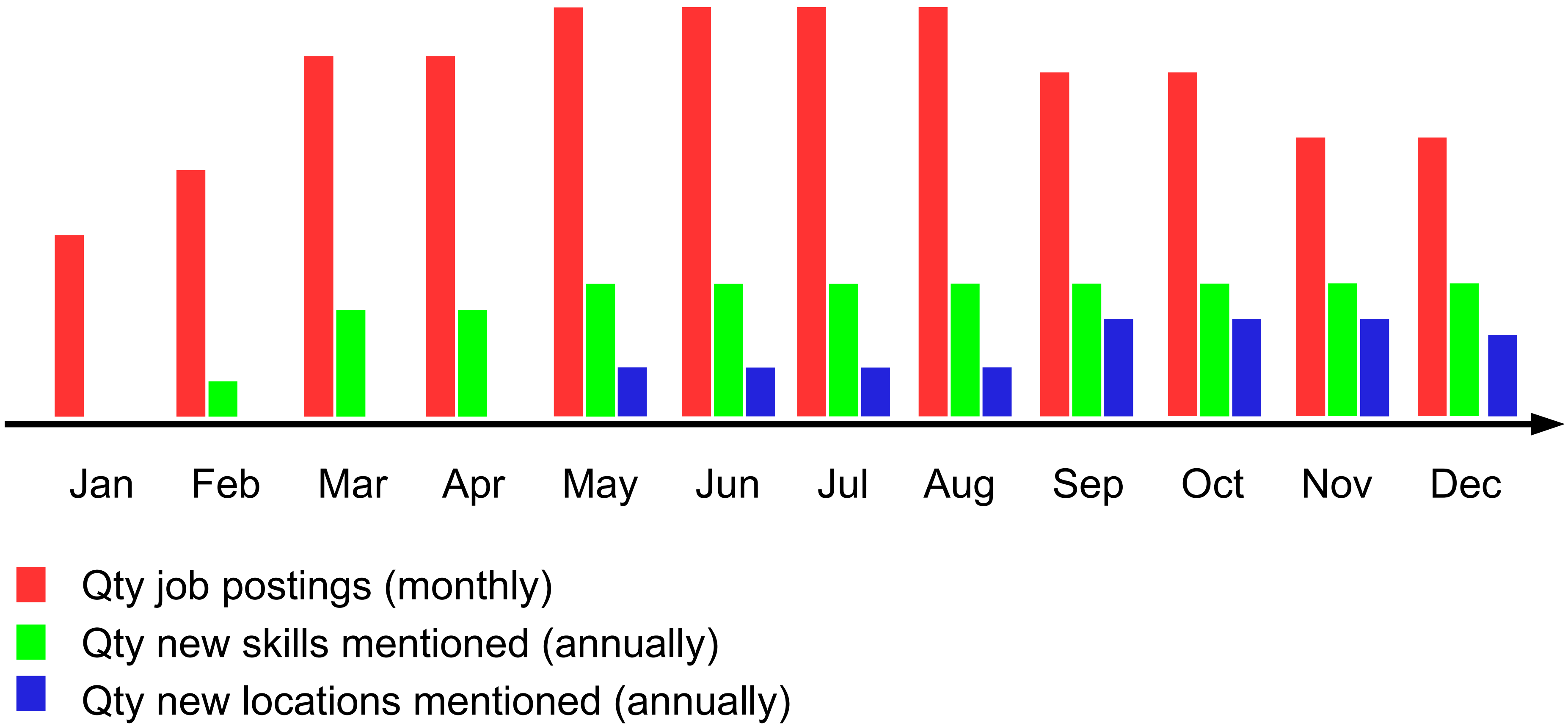
- High School Diploma/GED
- At least 1 year experience in Customer Service Experience
- At least 1 year experience in Technical Knowledge
- Portuguese: Fluent

Preferred

- English : Intermediate

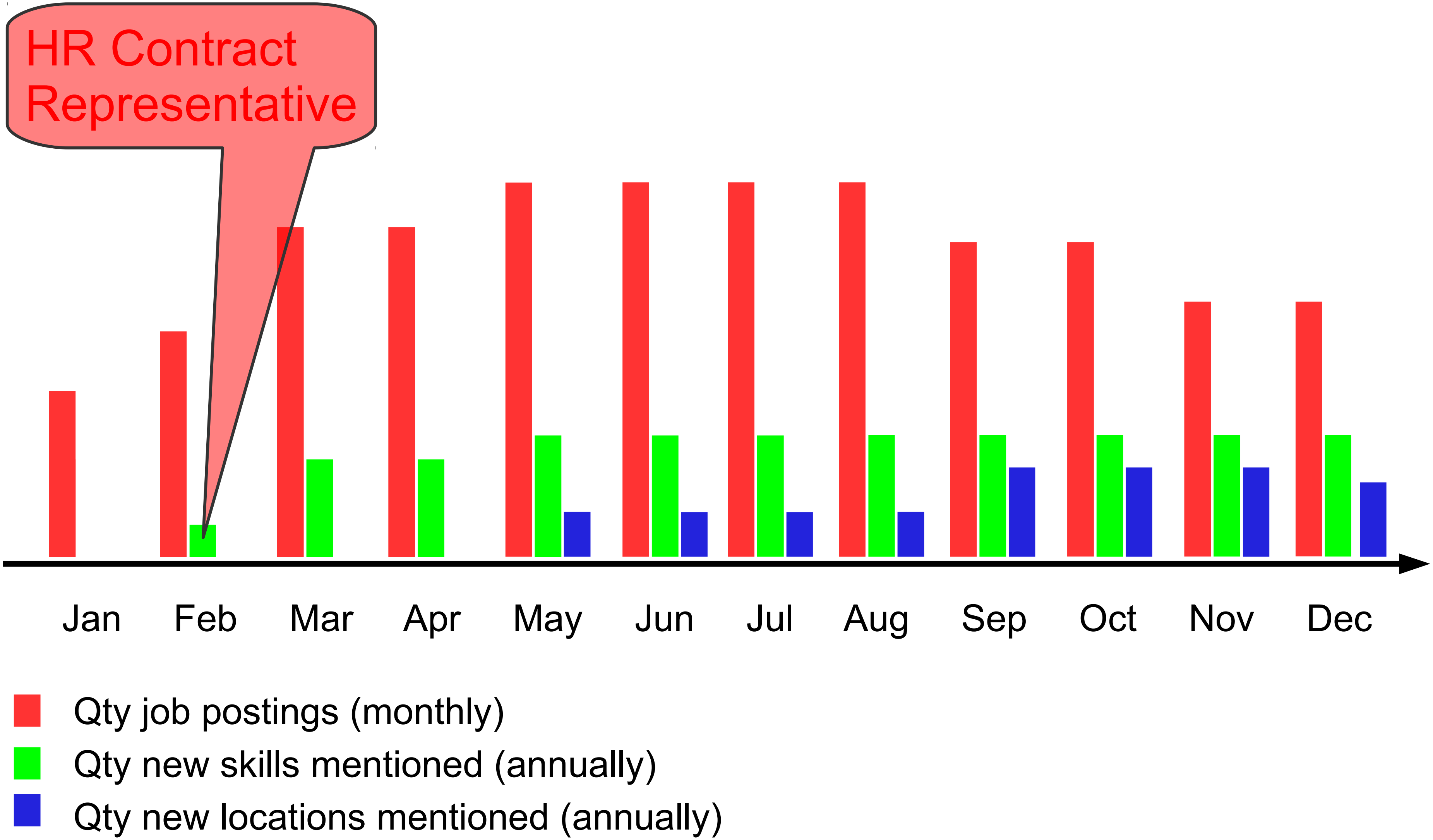
New Skill?

Monitored job postings leak strategic planning

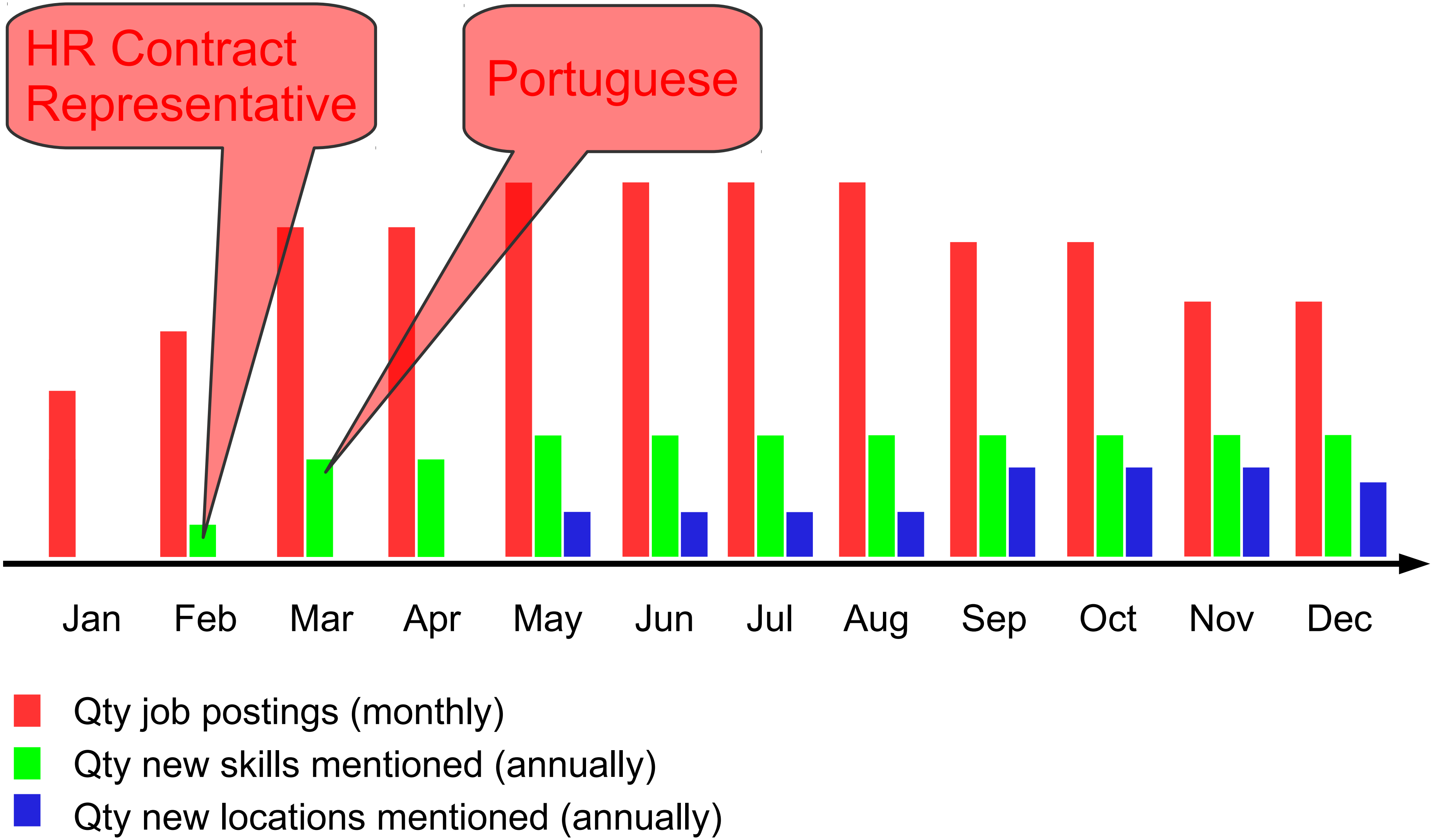


You're Leaking Trade Secrets

Monitored job postings leak strategic planning

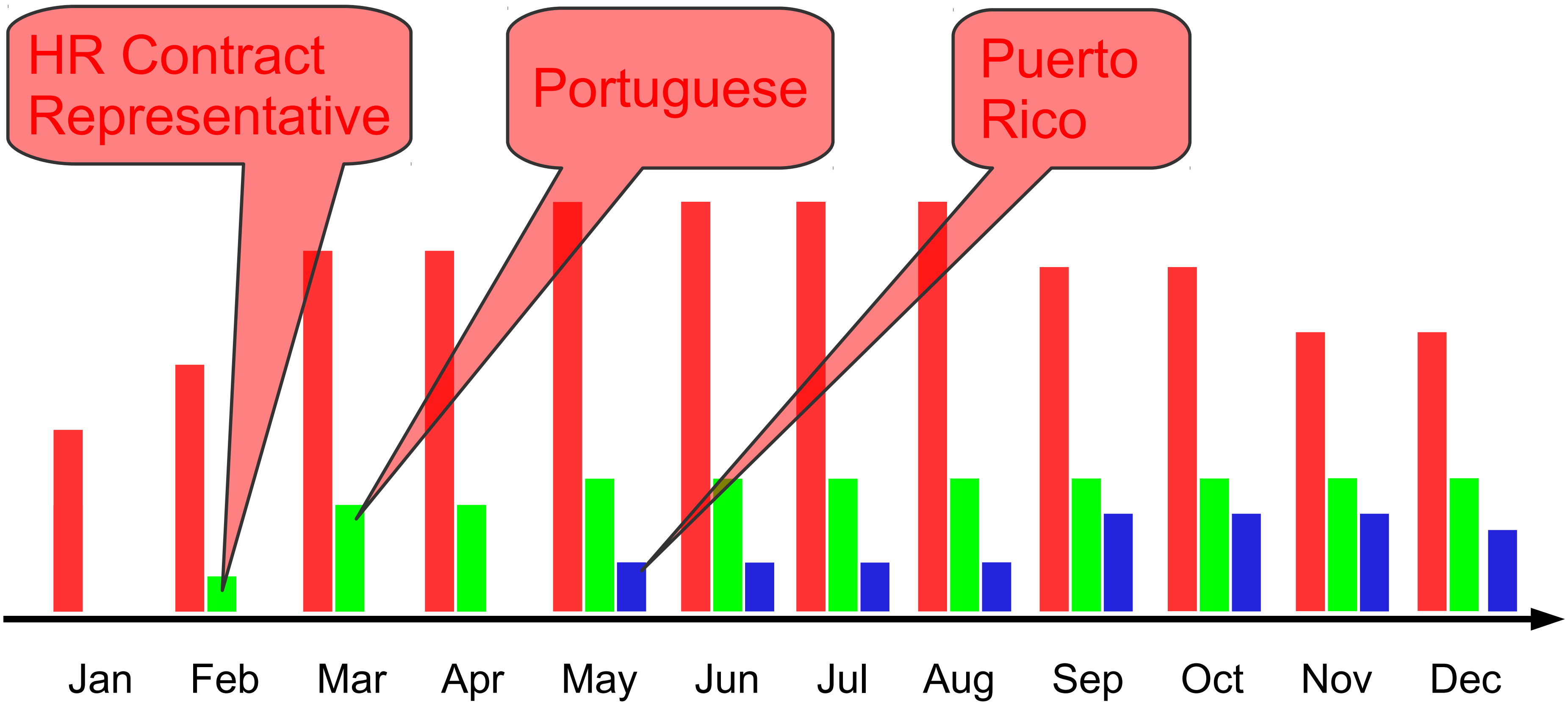


Monitored job postings leak strategic planning



🟥 Qty job postings (monthly)
🟩 Qty new skills mentioned (annually)
🟦 Qty new locations mentioned (annually)

Monitored job postings leak strategic planning



- 🟥 Qty job postings (monthly)
- 🟩 Qty new skills mentioned (annually)
- 🟦 Qty new locations mentioned (annually)

Monitored job postings leak strategic information

What HR thinks

I'm going to advertise the vacancy we have for an IT Help Desk professional.

What a hacker thinks

I can “read between the lines” to learn how to compromise a computer network, and discover trade secrets.

Monitored job postings leak strategic information

What HR thinks

I'm going to advertise the vacancy we have for an IT Help Desk professional.

What a hacker thinks

I can “read between the lines” to learn how to compromise a computer network, and discover trade secrets.

Job posting: Leaked security info

RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

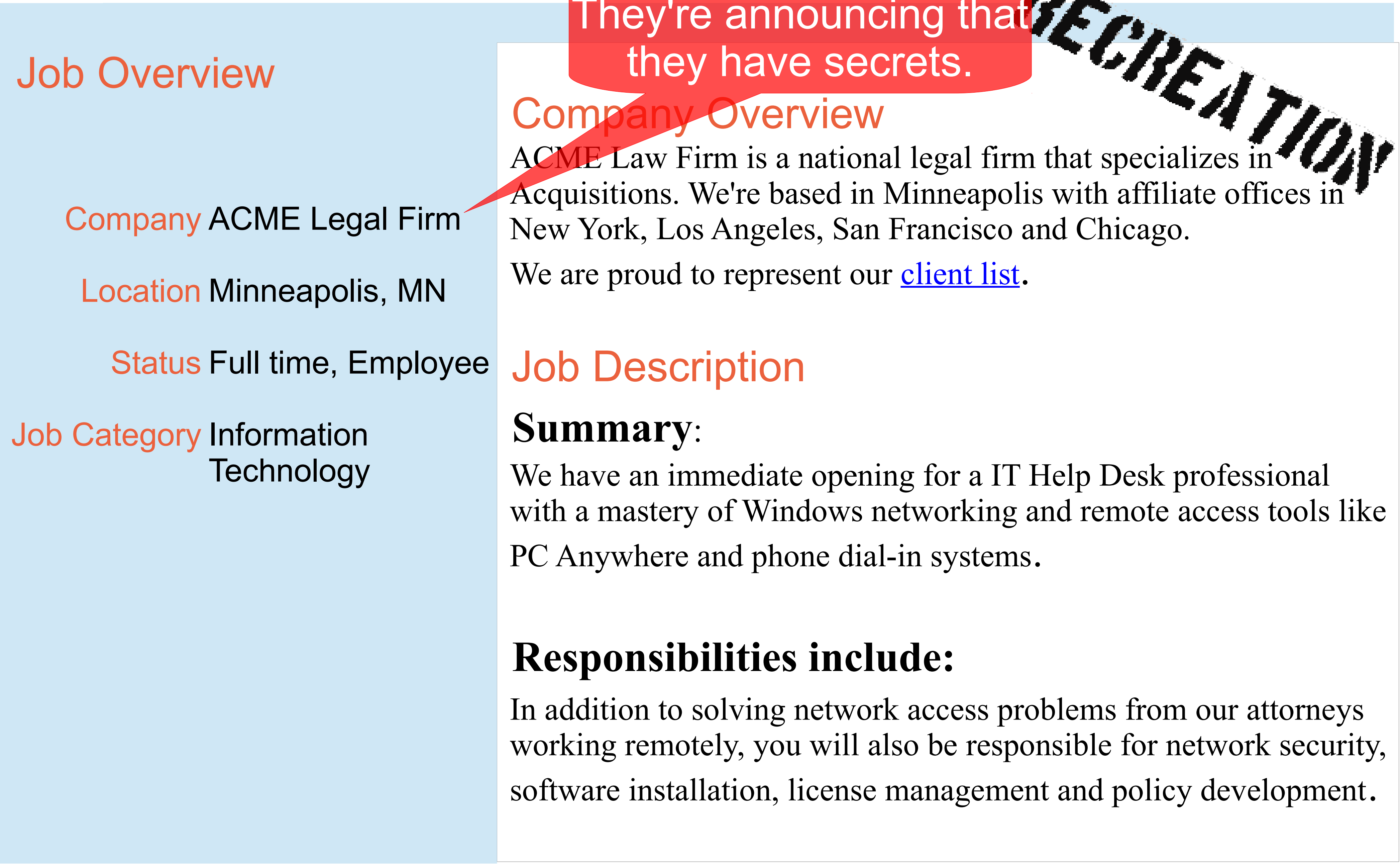
Summary:

We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

Job posting: Leaked security info



Job Overview

Company ACME Legal Firm

Location Minneapolis, MN

Status Full time, Employee

Job Category Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

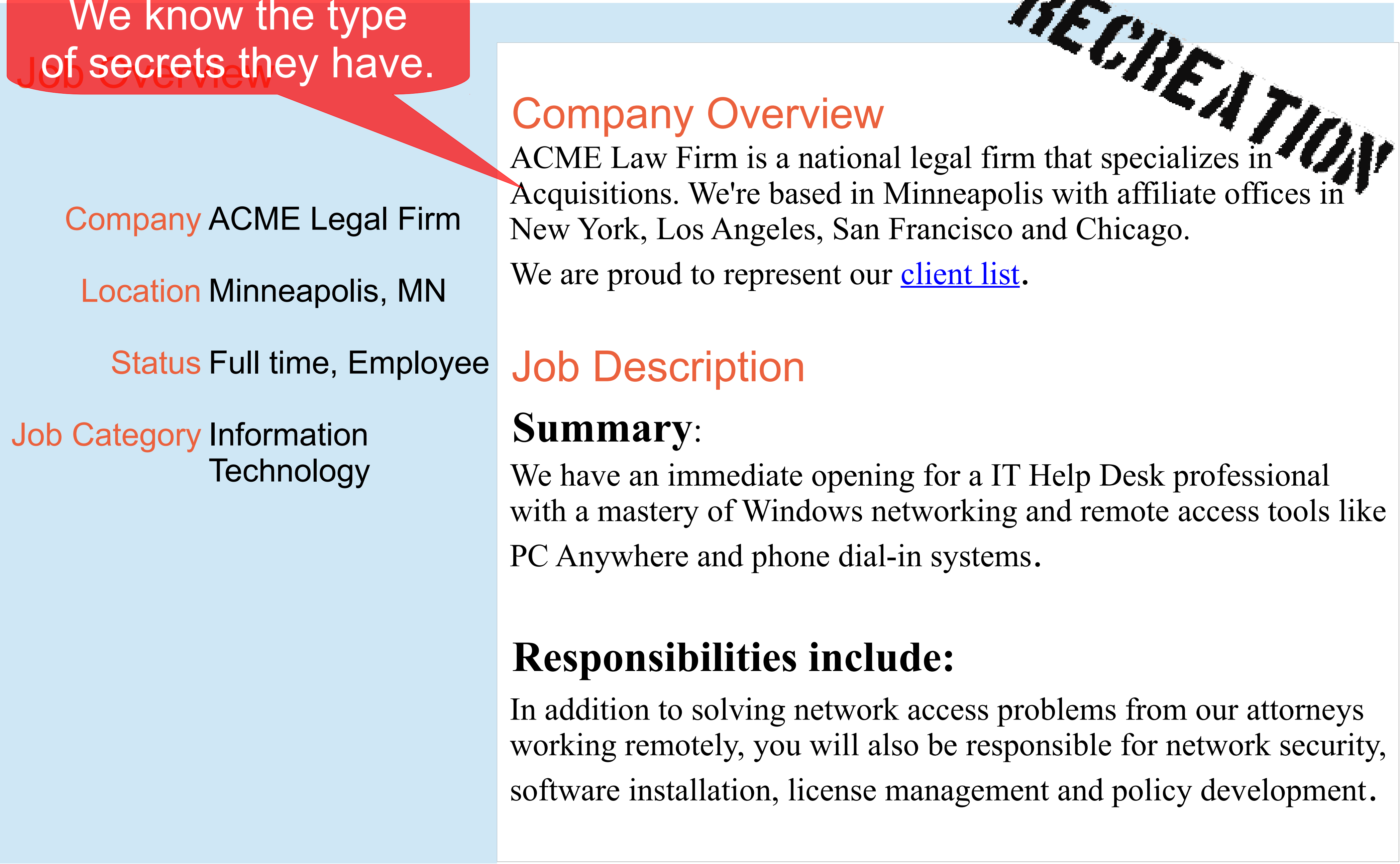
In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

They're announcing that they have secrets.

RECREATION

Job posting: Leaked security info

We know the type of secrets they have.



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

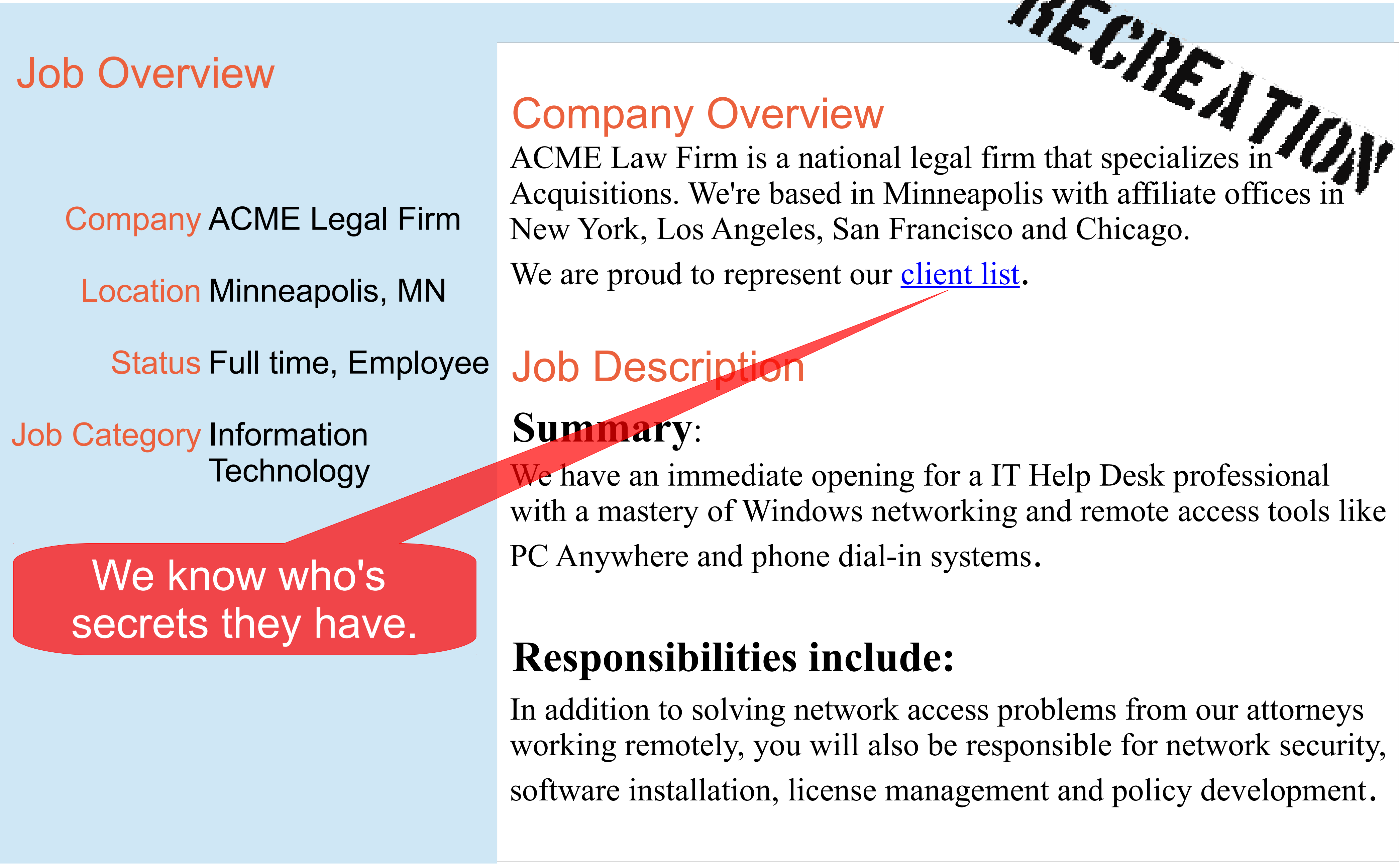
Summary:

We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

Job posting: Leaked security info



Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

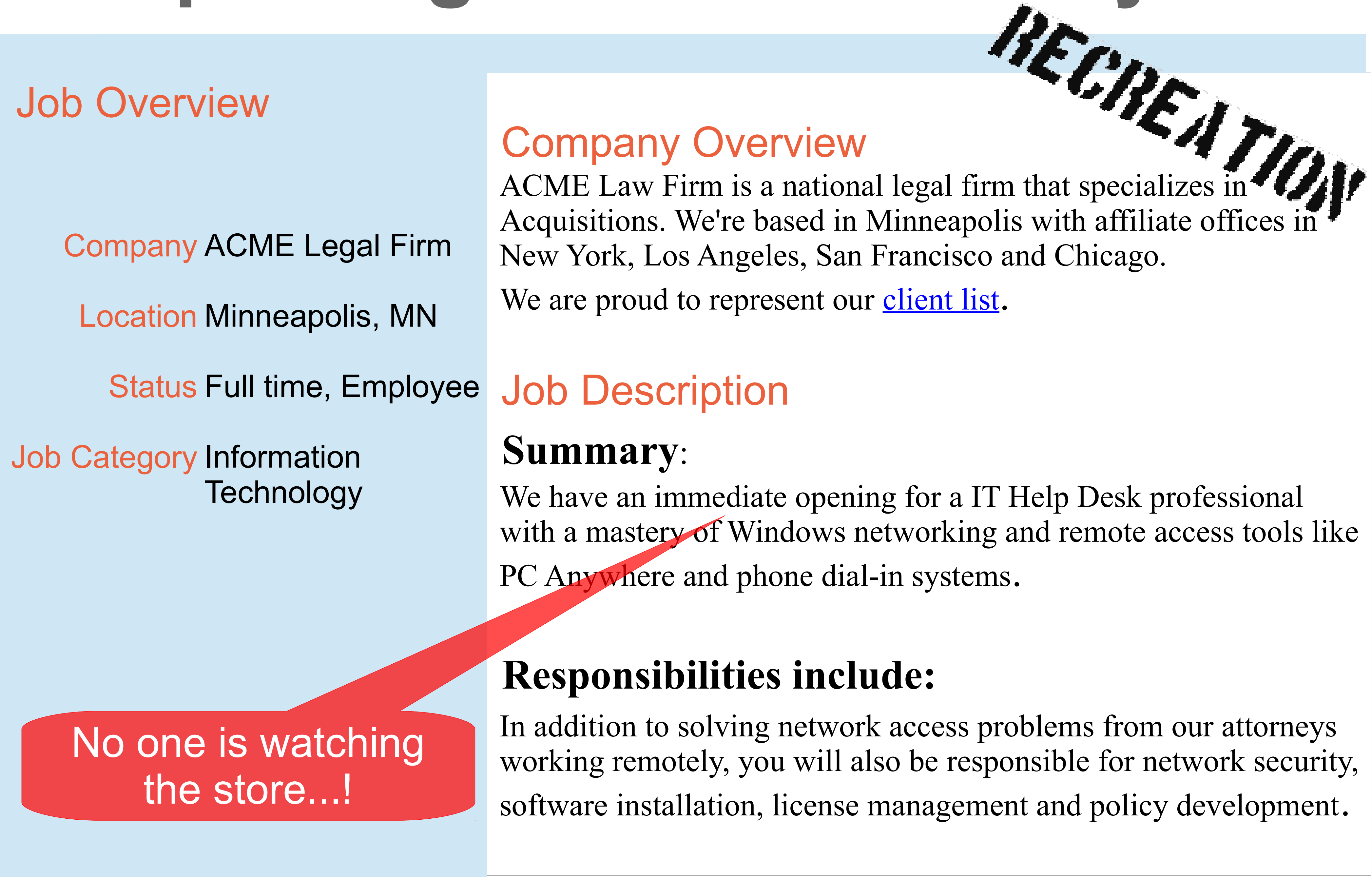
Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

RECREATION

We know who's secrets they have.

Job posting: Leaked security info



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

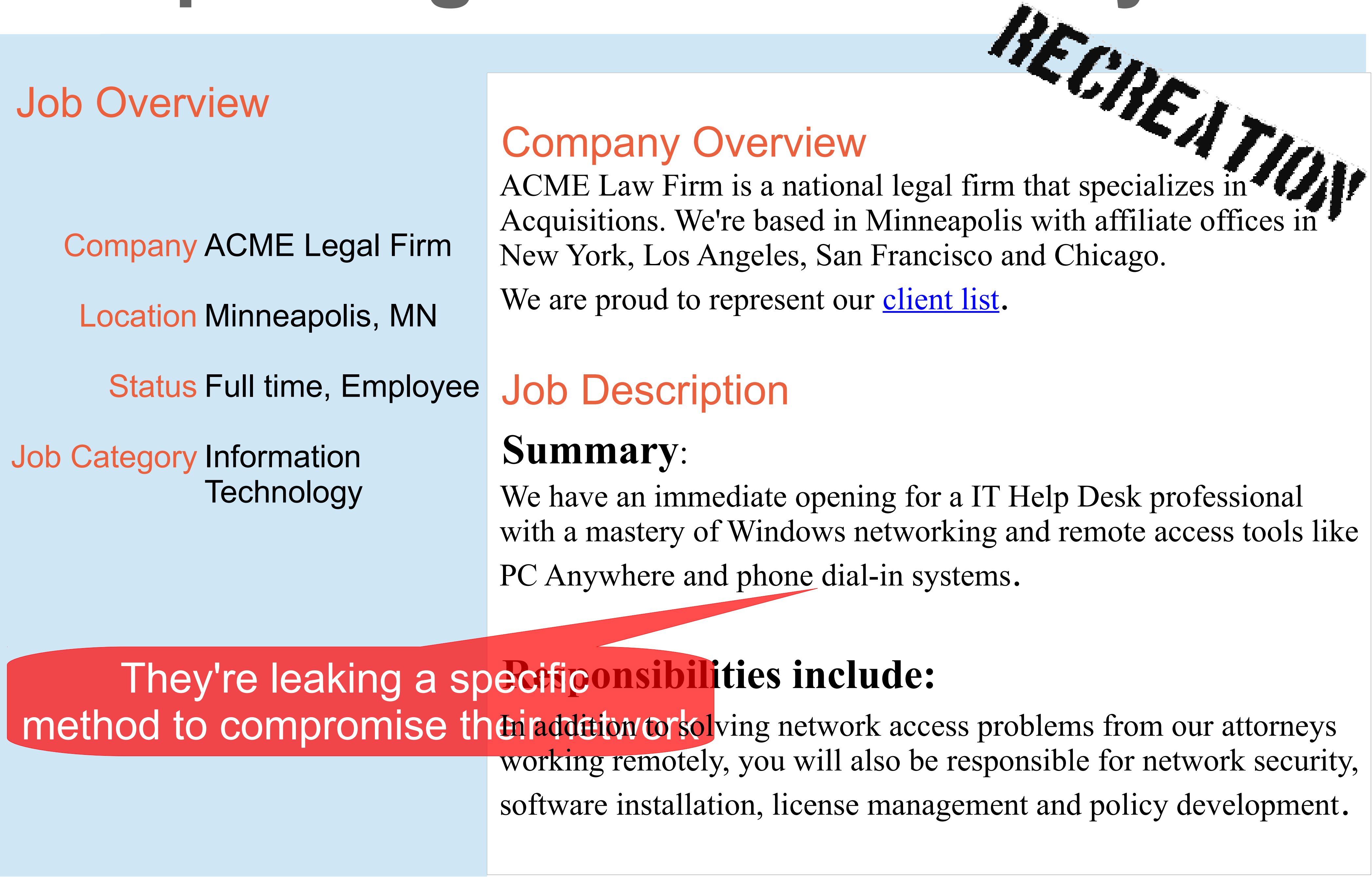
We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

No one is watching the store...!

Job posting: Leaked security info



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

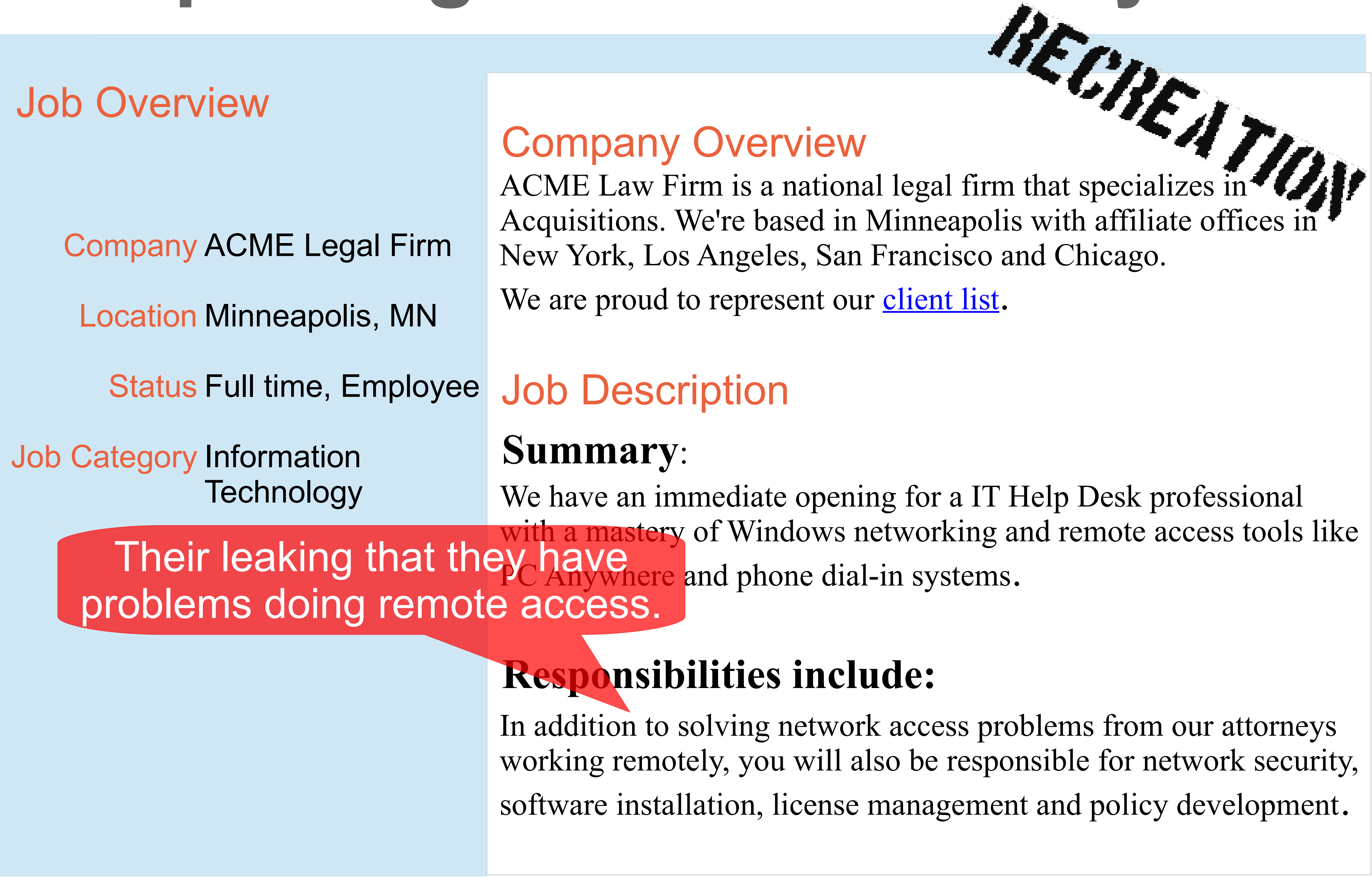
We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

They're leaking a specific method to compromise their network

Job posting: Leaked security info



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

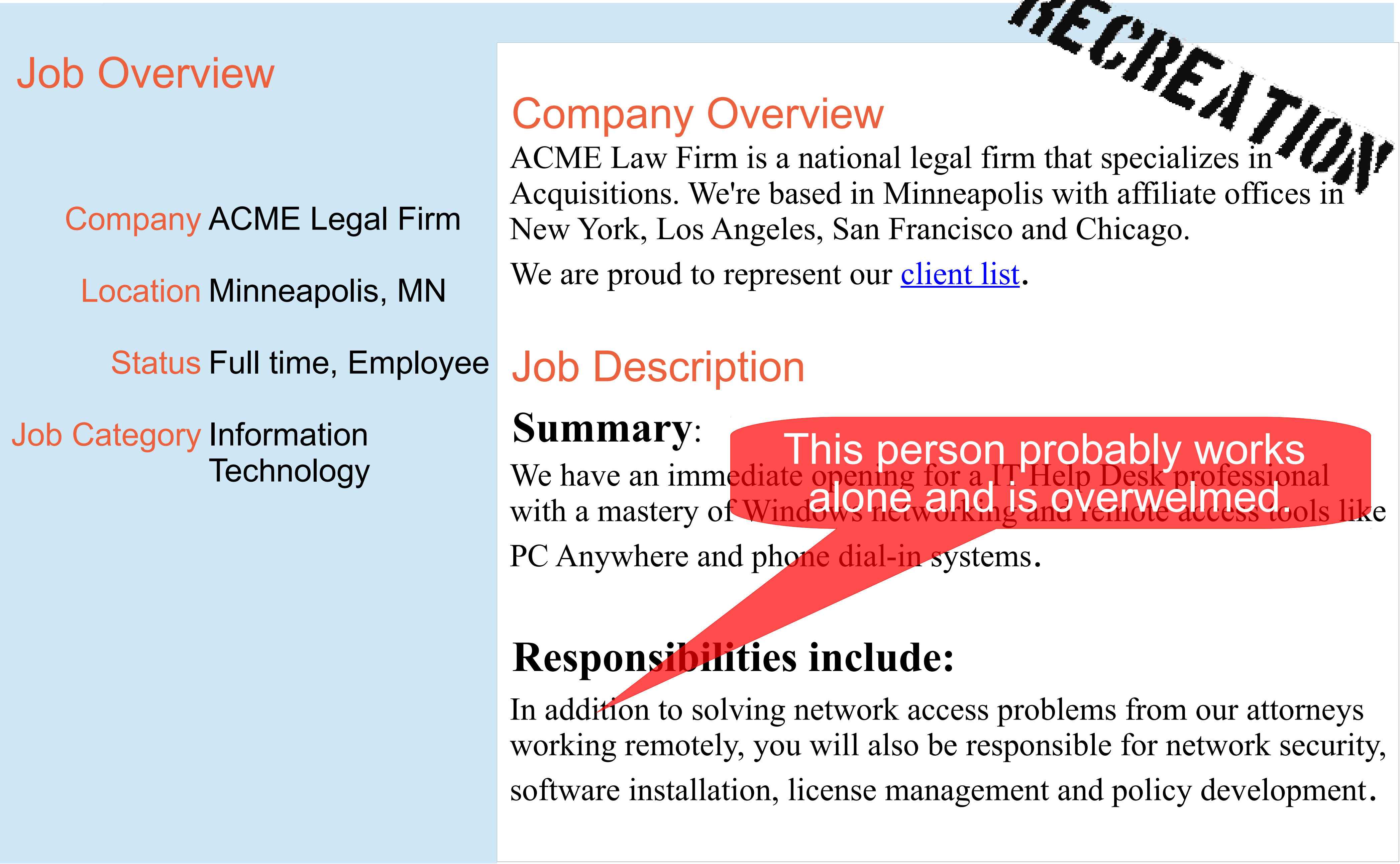
We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

Their leaking that they have problems doing remote access.

Job posting: Leaked security info



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

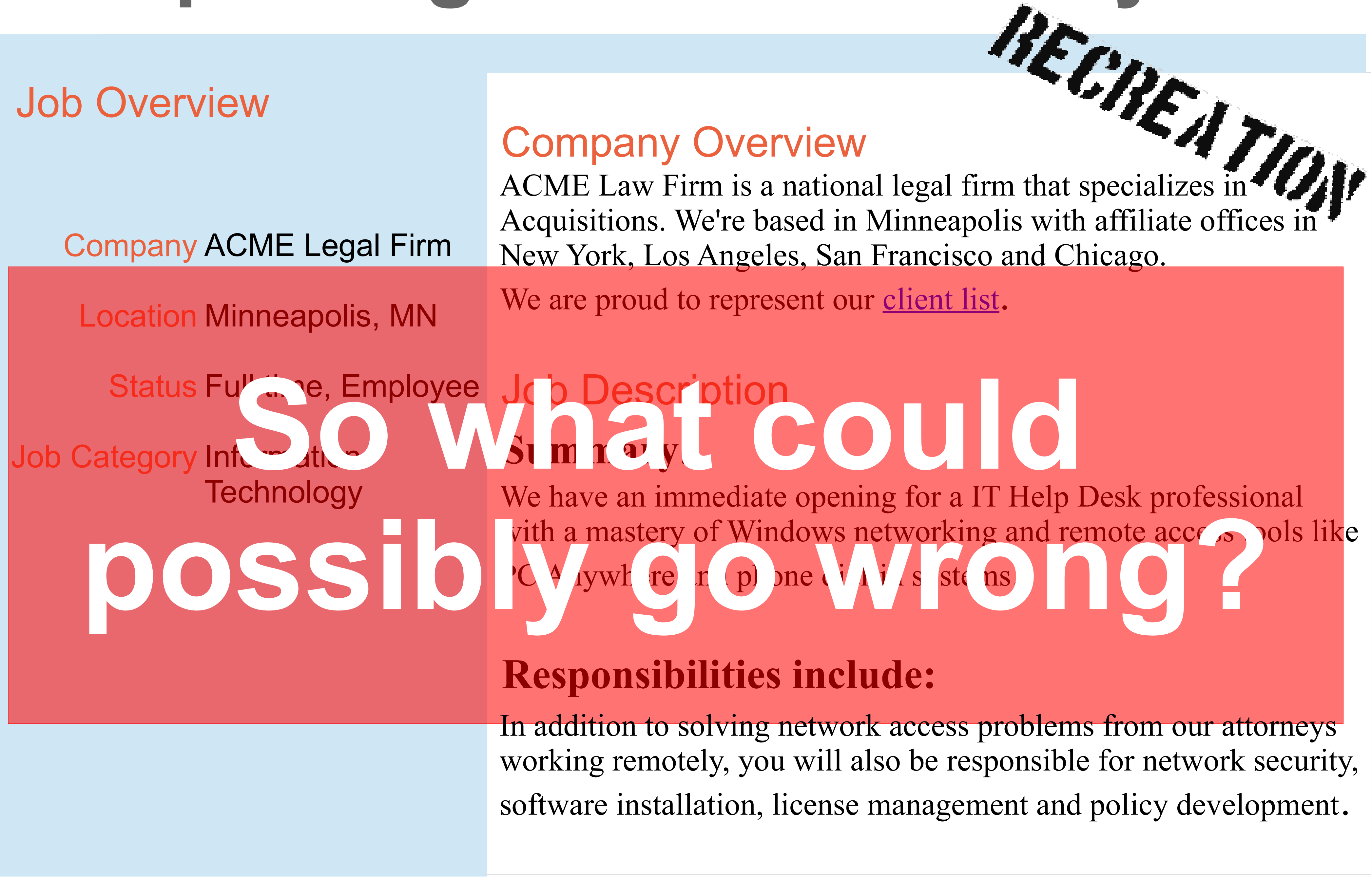
We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

This person probably works alone and is overwelmed.

Job posting: Leaked security info



RECREATION

Job Overview

Company	ACME Legal Firm
Location	Minneapolis, MN
Status	Full-time, Employee
Job Category	Information Technology

Company Overview

ACME Law Firm is a national legal firm that specializes in Acquisitions. We're based in Minneapolis with affiliate offices in New York, Los Angeles, San Francisco and Chicago.

We are proud to represent our client list.

Job Description

Summary:

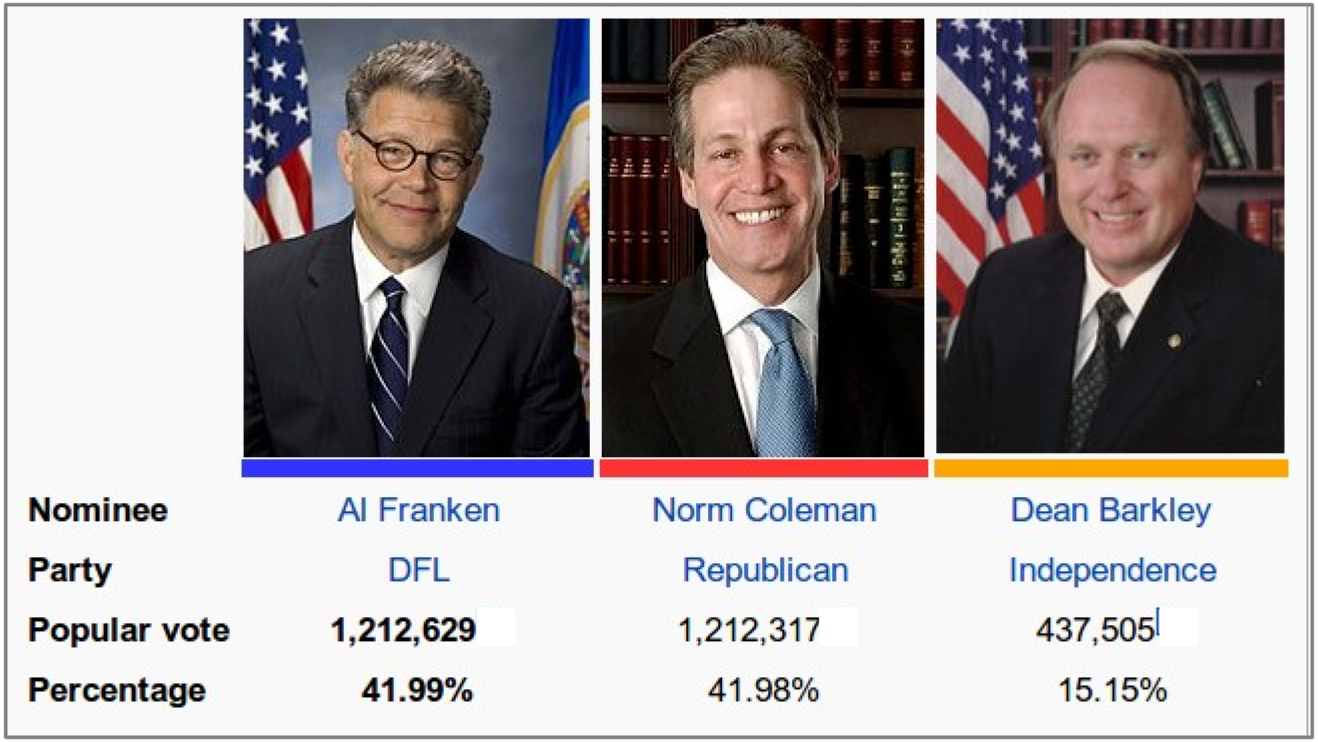
We have an immediate opening for a IT Help Desk professional with a mastery of Windows networking and remote access tools like PC Anywhere and phone dial-in systems.

Responsibilities include:

In addition to solving network access problems from our attorneys working remotely, you will also be responsible for network security, software installation, license management and policy development.

So what could possibly go wrong?

Sometimes databases are left in plain sight (MN Senatorial election 2006)

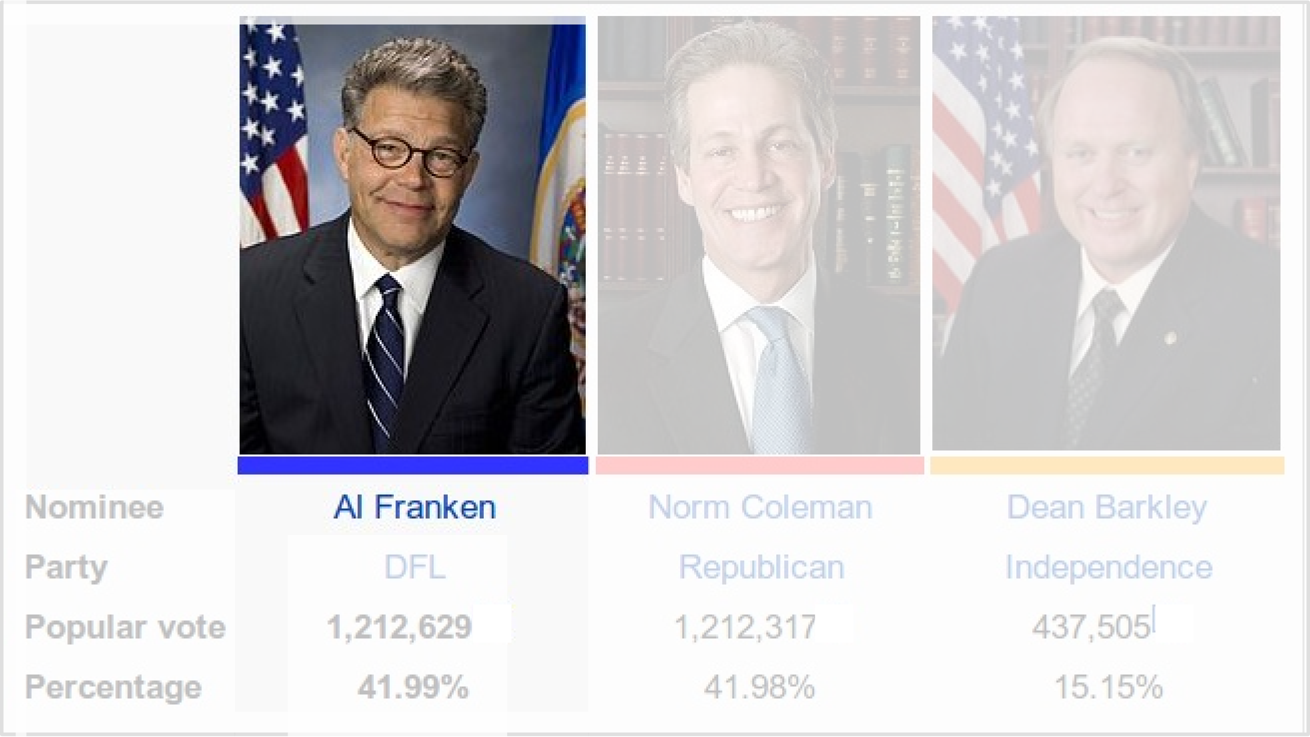


Nominee	Al Franken	Norm Coleman	Dean Barkley
Party	DFL	Republican	Independence
Popular vote	**1,212,629**	1,212,317	437,505
Percentage	**41.99%**	41.98%	15.15%

This was an extremely close election
Any leaked secrets could change the outcome

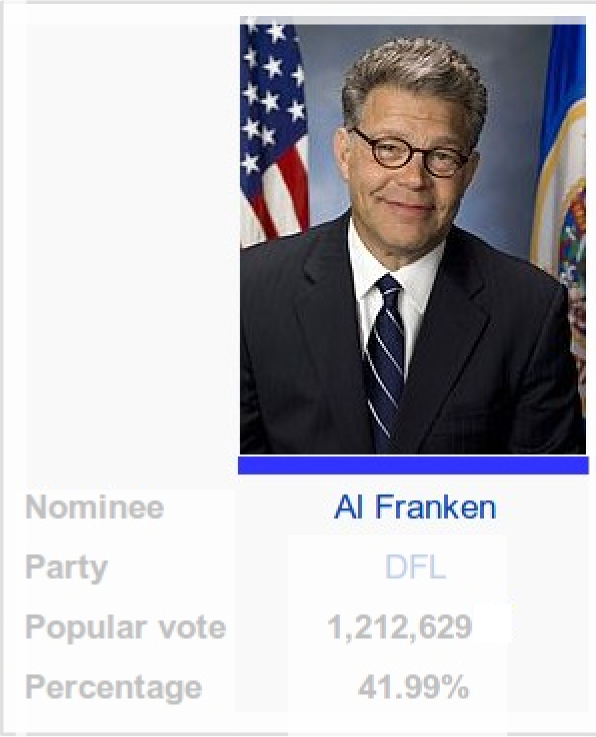
You're Leaking Trade Secrets

Sometimes databases are left in plain sight (MN Senatorial election 2006)



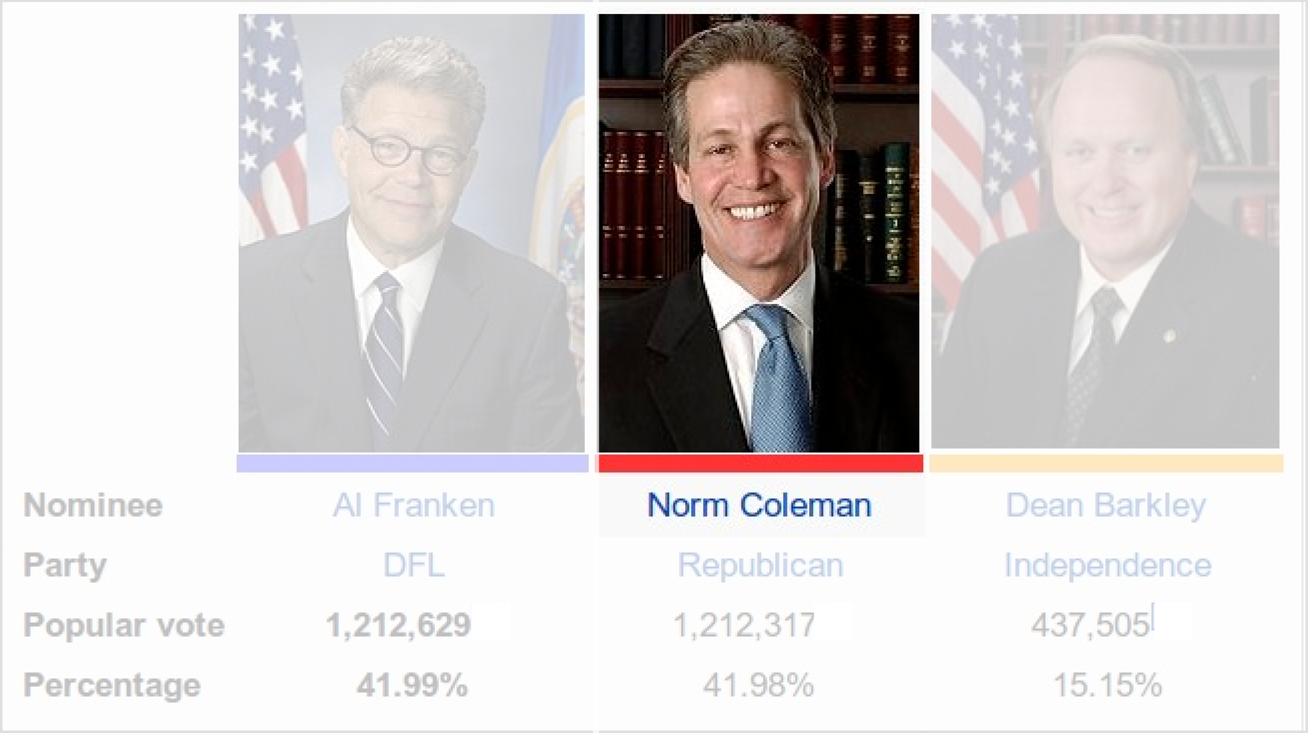
Nominee	Al Franken	Norm Coleman	Dean Barkley
Party	DFL	Republican	Independence
Popular vote	1,212,629	1,212,317	437,505
Percentage	41.99%	41.98%	15.15%

Sometimes databases are left in plain sight (MN Senatorial election 2006)



Nominee	Al Franken
Party	DFL
Popular vote	1,212,629
Percentage	41.99%

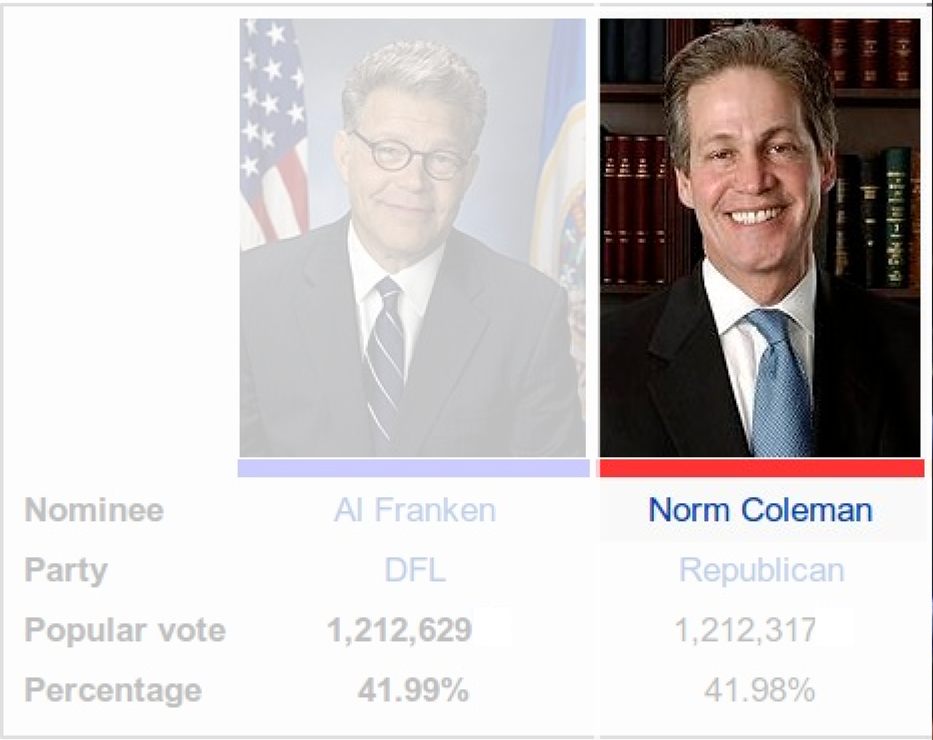
Sometimes databases are left in plain sight (MN Senatorial election 2006)



Nominee	Al Franken	Norm Coleman	Dean Barkley
Party	DFL	Republican	Independence
Popular vote	1,212,629	1,212,317	437,505
Percentage	41.99%	41.98%	15.15%

You're Leaking Trade Secrets

Sometimes databases are left in plain sight (MN Senatorial election 2006)



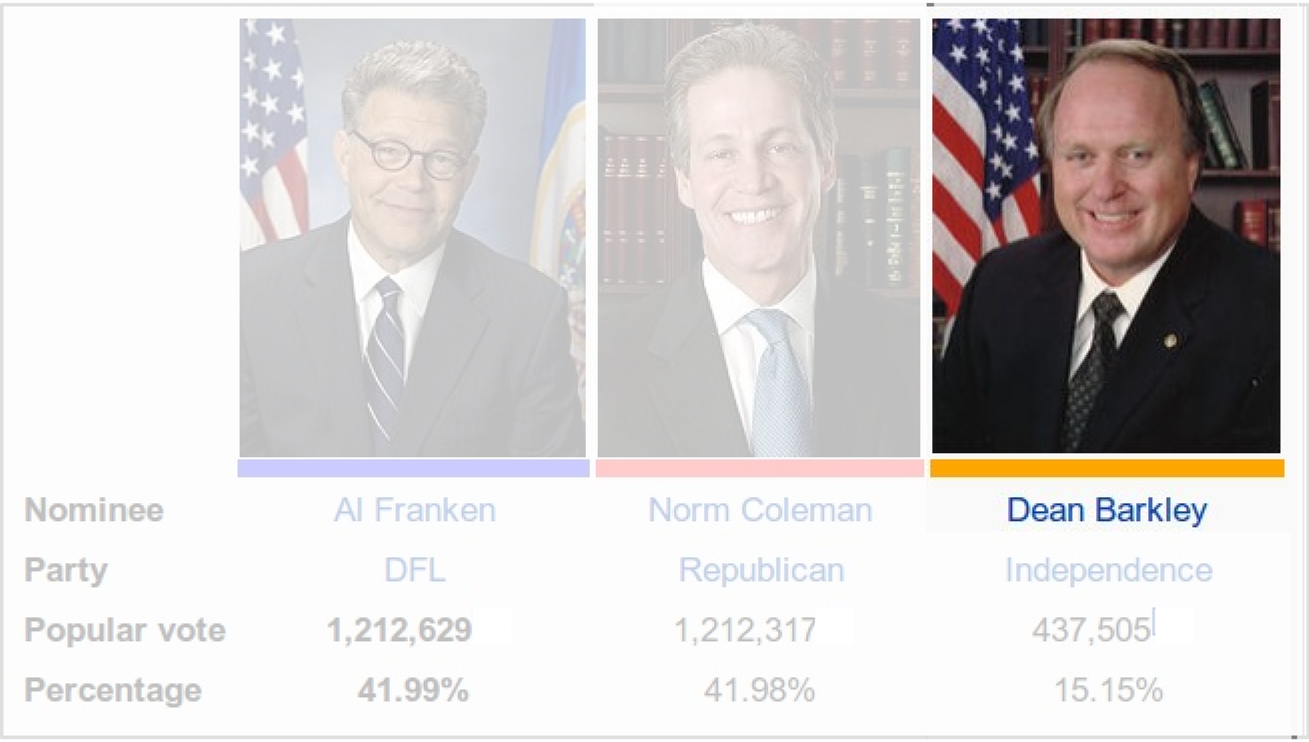
Nominee	Al Franken	Norm Coleman
Party	DFL	Republican
Popular vote	1,212,629	1,212,317
Percentage	41.99%	41.98%

Jesse Ventura

You're Leaking Trade Secrets

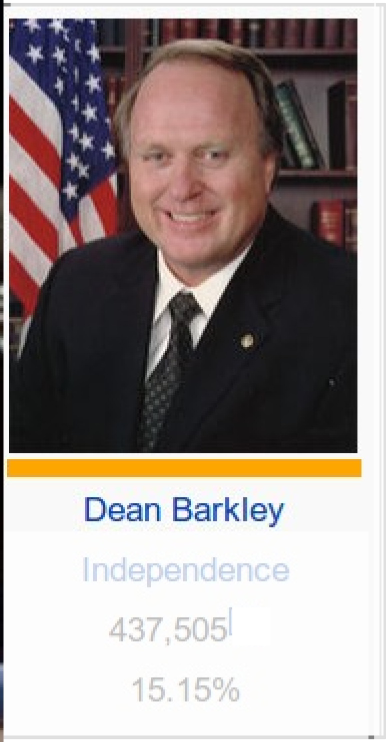
You're Leaking Trade Secrets

Sometimes databases are left in plain sight (MN Senatorial election 2006)



Nominee	Al Franken	Norm Coleman	Dean Barkley
Party	DFL	Republican	Independence
Popular vote	**1,212,629**	1,212,317	437,505
Percentage	**41.99%**	41.98%	15.15%

Sometimes databases are left in plain sight (MN Senatorial election 2006)

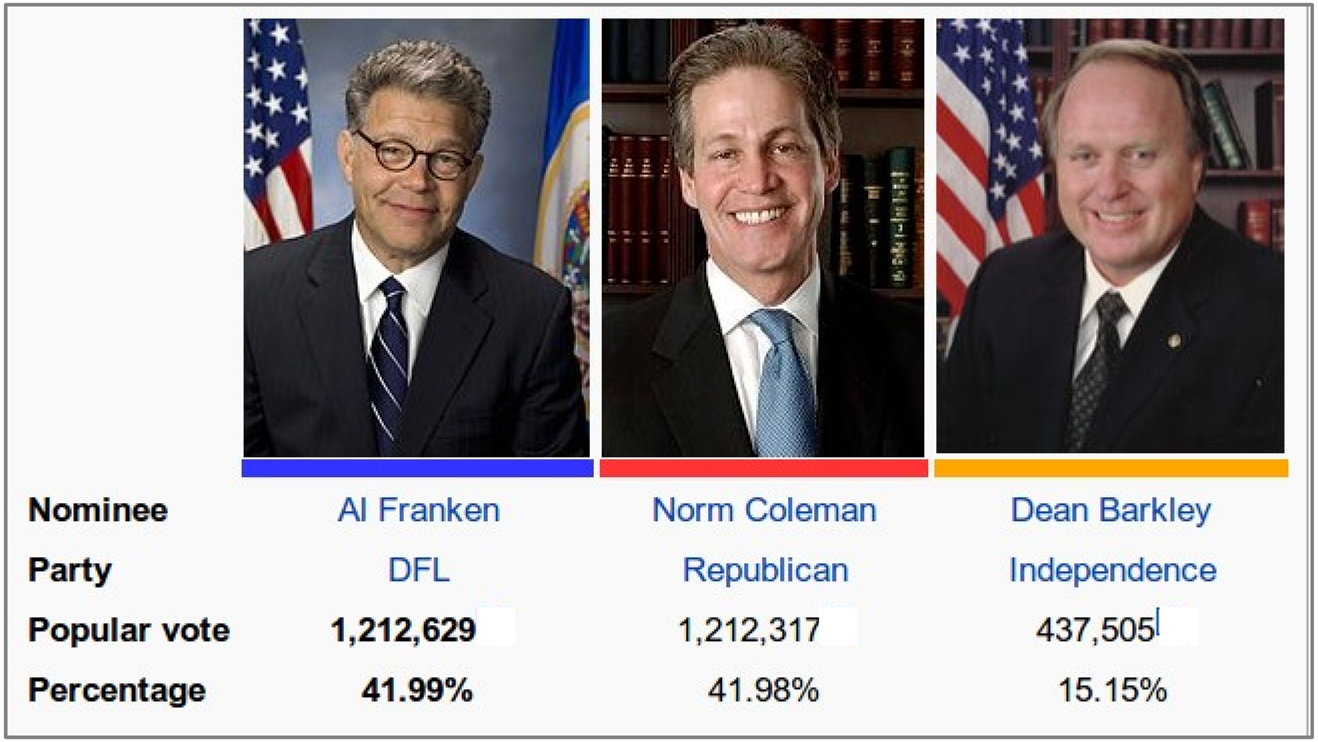

Dean Barkley

Independence

437,505

15.15%

Sometimes databases are left in plain sight (MN Senatorial election 2006)

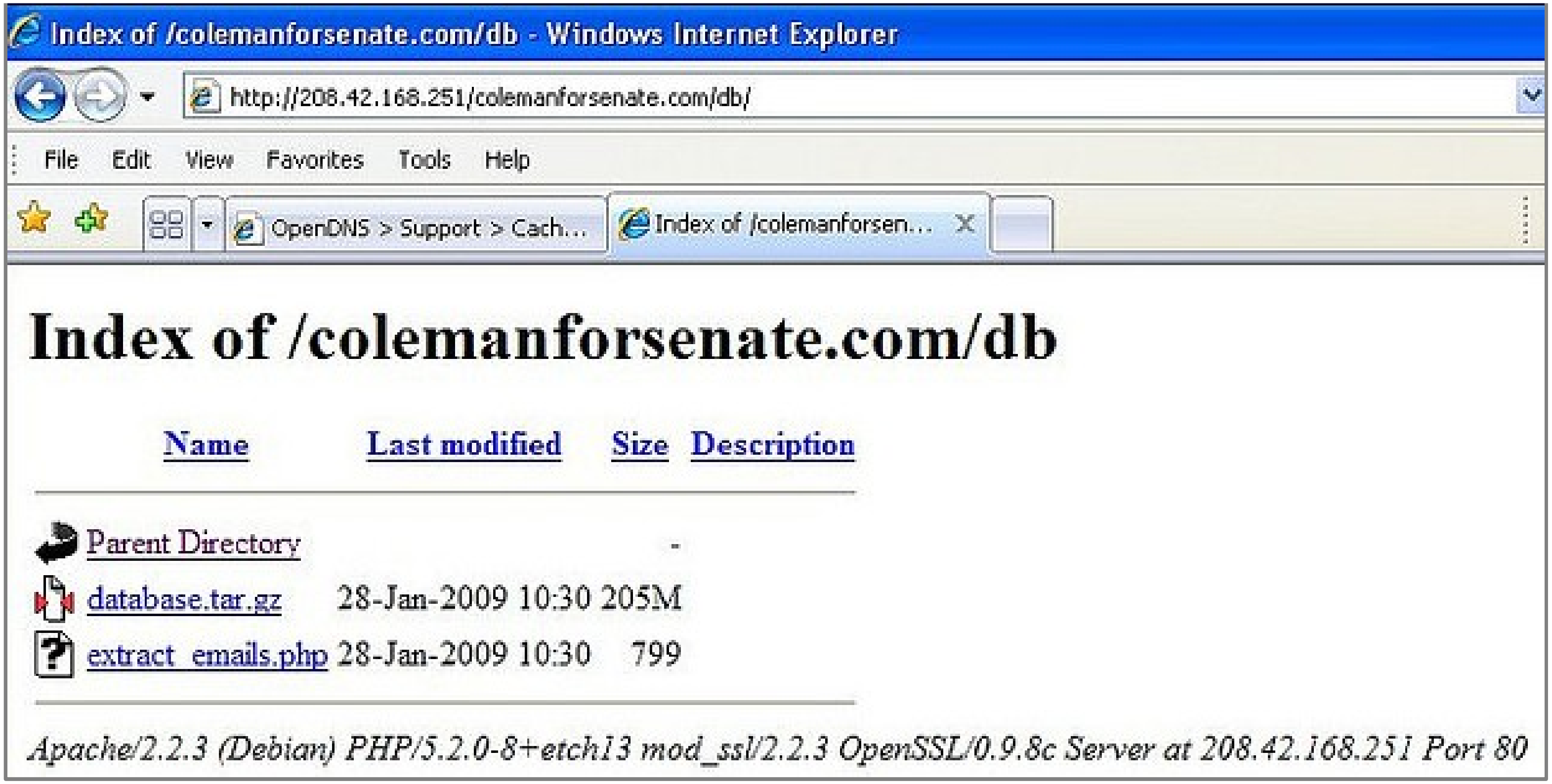


Nominee	Al Franken	Norm Coleman	Dean Barkley
Party	DFL	Republican	Independence
Popular vote	**1,212,629**	1,212,317	437,505
Percentage	**41.99%**	41.98%	15.15%

Al Franken defeated **Norm Coleman** by 312 votes *(after six months in court) court*

There were multiple charges of hacking made by the Coleman campaign prior to the election

Sometimes databases are left in plain sight (MN Senatorial election 2006)


Index of /colemanforsenate.com/db - Windows Internet Explorer
http://208.42.168.251/colemanforsenate.com/db/
File
Edit
View
Favorites
Tools
Help
OpenDNS > Support > Cach...
Index of /colemanforsen...

Index of /colemanforsenate.com/db

Name	Last modified	Size	Description
Parent Directory		-	
database.tar.gz	28-Jan-2009 10:30	205M	
extract_emails.php	28-Jan-2009 10:30	799	

Apache/2.2.3 (Debian) PHP/5.2.0-8+etch13 mod_ssl/2.2.3 OpenSSL/0.9.8c Server at 208.42.168.251 Port 80

The Coleman campaign left a database of donors (and their credit card numbers) sitting in an unprotected directory of their web server*.

*Adria Richards

Monitored DNS records leak future strategic plans

What Marketing thinks

I need to register domain names for a new products

What a hacker thinks

I can watch DNS registrations remotely

I can be anonymous

I can automate the information gathering

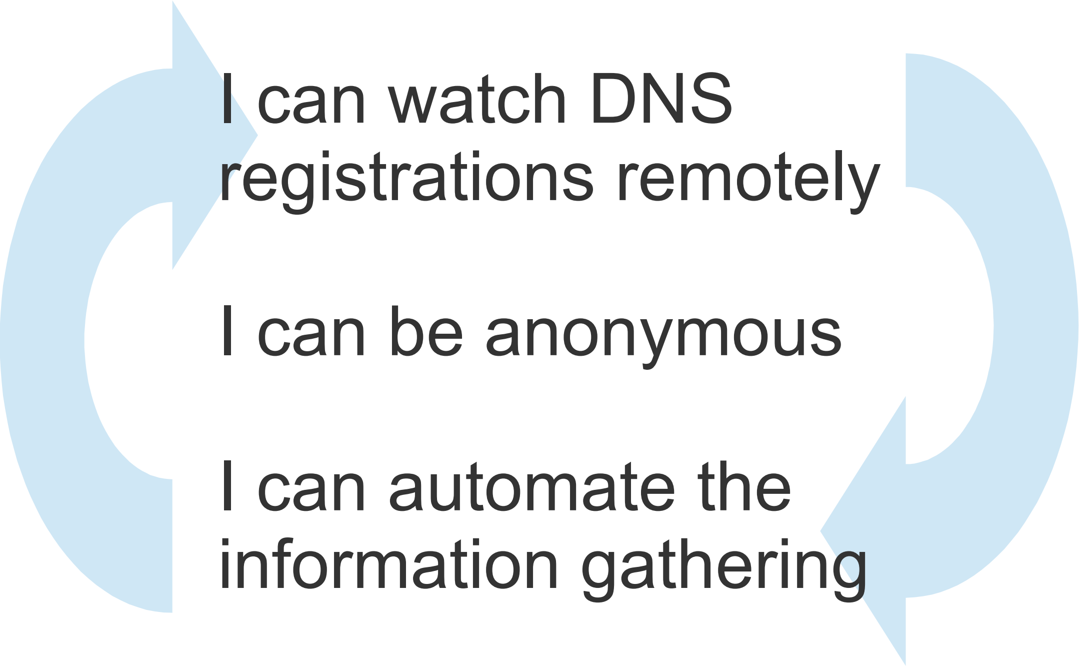
You're Leaking Trade Secrets

Monitored DNS records leak future strategic plans

What Marketing thinks

I need to register domain names for a new products

What a hacker thinks



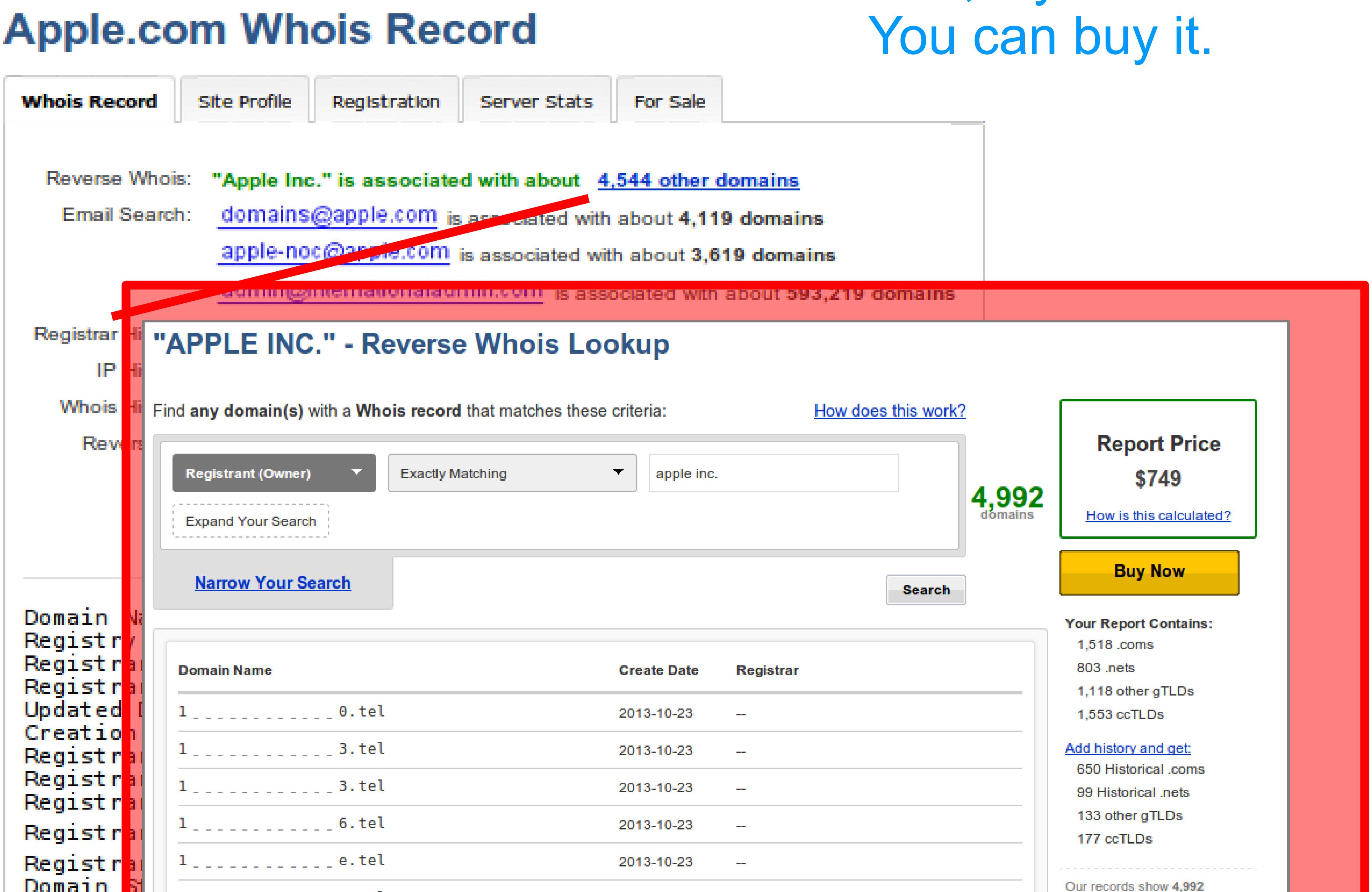
I can watch DNS registrations remotely

I can be anonymous

I can automate the information gathering

Monitored DNS records leak future strategic plans

And, if you can't hack it,
You can buy it.



Apple.com Whois Record

Reverse Whois: "Apple Inc." is associated with about 4,544 other domains

Email Search: domains@apple.com is associated with about 4,119 domains

apple-noc@apple.com is associated with about 3,619 domains

admin@internationaladmin.com is associated with about 593,219 domains

Registrar Hi

IP Hi

Whois Hi

Rev

Domain Na
Registr
Registr
Registr
Updated
Creatio
Registr
Registr
Registr
Registr
Registr
Domain St

"APPLE INC." - Reverse Whois Lookup

Find **any domain(s)** with a **Whois record** that matches these criteria: How does this work?

4,992 domains

Report Price
$749
How is this calculated?

Domain Name	Create Date	Registrar
1 _ _ _ _ _ _ _ _ _ _ _ _ 0.tel	2013-10-23	--
1 _ _ _ _ _ _ _ _ _ _ _ _ 3.tel	2013-10-23	--
1 _ _ _ _ _ _ _ _ _ _ _ _ 3.tel	2013-10-23	--
1 _ _ _ _ _ _ _ _ _ _ _ _ 6.tel	2013-10-23	--
1 _ _ _ _ _ _ _ _ _ _ _ _ e.tel	2013-10-23	--

Your Report Contains:
1,518 .coms
803 .nets
1,118 other gTLDs
1,553 ccTLDs

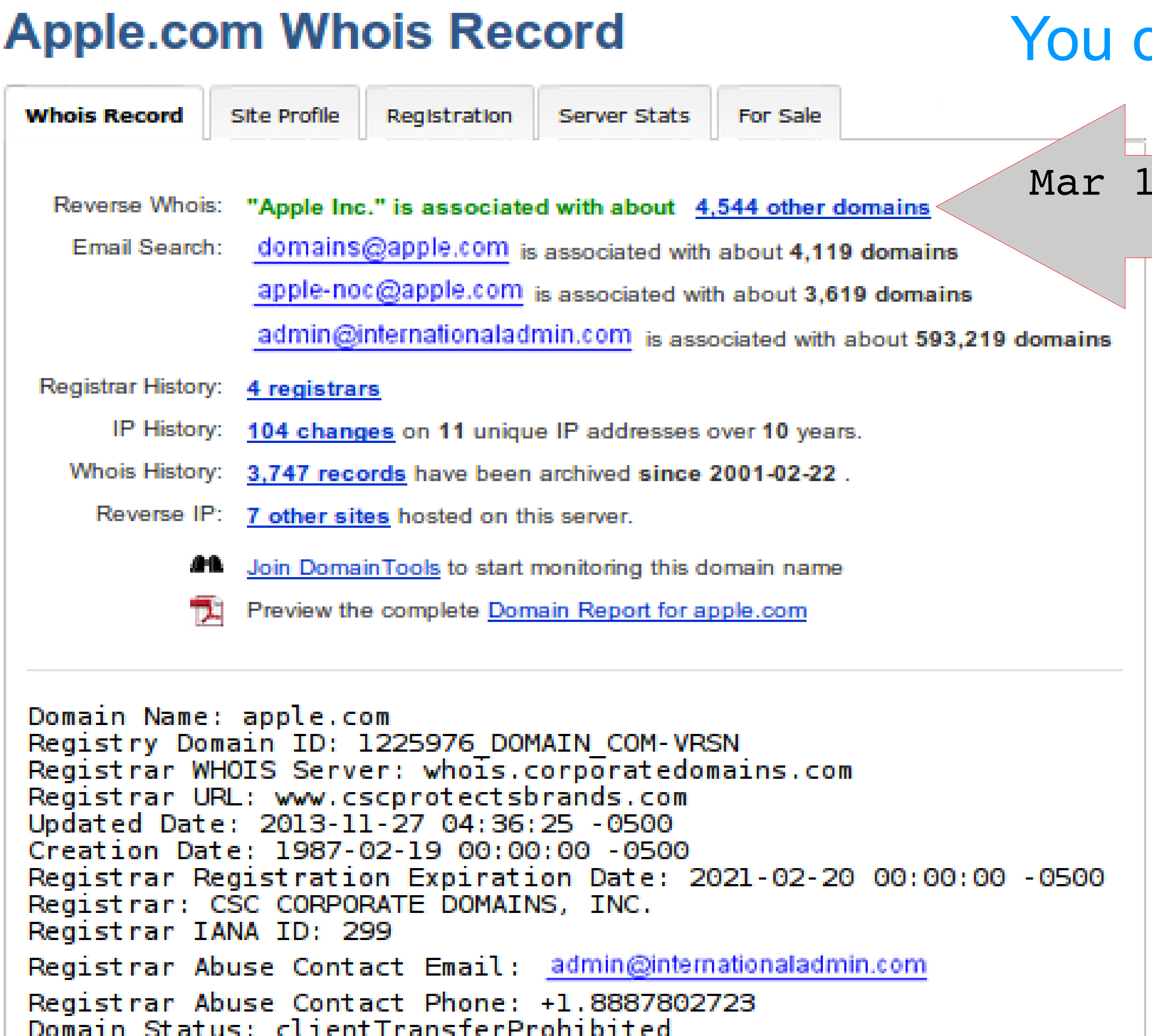
Add history and get:
650 Historical .coms
99 Historical .nets
133 other gTLDs
177 ccTLDs

Our records show 4,992

You're Leaking Trade Secrets

Monitored DNS records leak future strategic plans

And, if you can't hack it,
You can buy it.



Apple.com Whois Record

Reverse Whois: "Apple Inc." is associated with about 4,544 other domains

Email Search: domains@apple.com is associated with about 4,119 domains

apple-noc@apple.com is associated with about 3,619 domains

admin@internationaladmin.com is associated with about 593,219 domains

Registrar History: 4 registrars

IP History: 104 changes on 11 unique IP addresses over 10 years.

Whois History: 3,747 records have been archived since 2001-02-22 .

Reverse IP: 7 other sites hosted on this server.

Join DomainTools to start monitoring this domain name

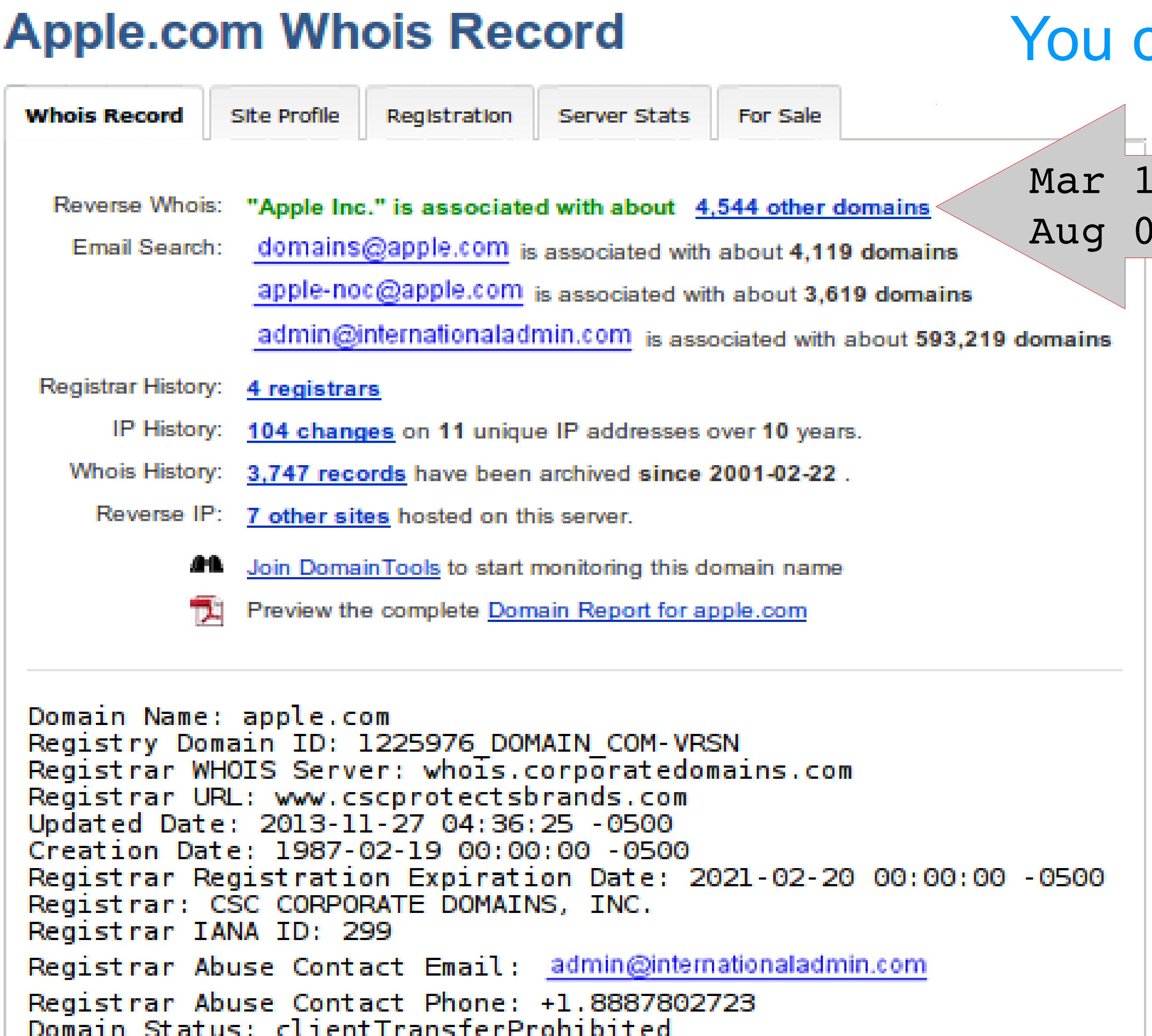
Preview the complete Domain Report for apple.com

```
Domain Name: apple.com
Registry Domain ID: 1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2013-11-27 04:36:25 -0500
Creation Date: 1987-02-19 00:00:00 -0500
Registrar Registration Expiration Date: 2021-02-20 00:00:00 -0500
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: admin@internationaladmin.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited
```

Mar 17, 2014, 4544 domains

Monitored DNS records leak future strategic plans

And, if you can't hack it,
You can buy it.



Apple.com Whois Record

Reverse Whois: "Apple Inc." is associated with about 4,544 other domains

Email Search: domains@apple.com is associated with about 4,119 domains
apple-noc@apple.com is associated with about 3,619 domains
admin@internationaladmin.com is associated with about 593,219 domains

Registrar History: 4 registrars

IP History: 104 changes on 11 unique IP addresses over 10 years.

Whois History: 3,747 records have been archived since 2001-02-22 .

Reverse IP: 7 other sites hosted on this server.

Join DomainTools to start monitoring this domain name

Preview the complete Domain Report for apple.com

```
Domain Name: apple.com
Registry Domain ID: 1225976_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.corporatedomains.com
Registrar URL: www.cscprotectsbrands.com
Updated Date: 2013-11-27 04:36:25 -0500
Creation Date: 1987-02-19 00:00:00 -0500
Registrar Registration Expiration Date: 2021-02-20 00:00:00 -0500
Registrar: CSC CORPORATE DOMAINS, INC.
Registrar IANA ID: 299
Registrar Abuse Contact Email: admin@internationaladmin.com
Registrar Abuse Contact Phone: +1.8887802723
Domain Status: clientTransferProhibited
```

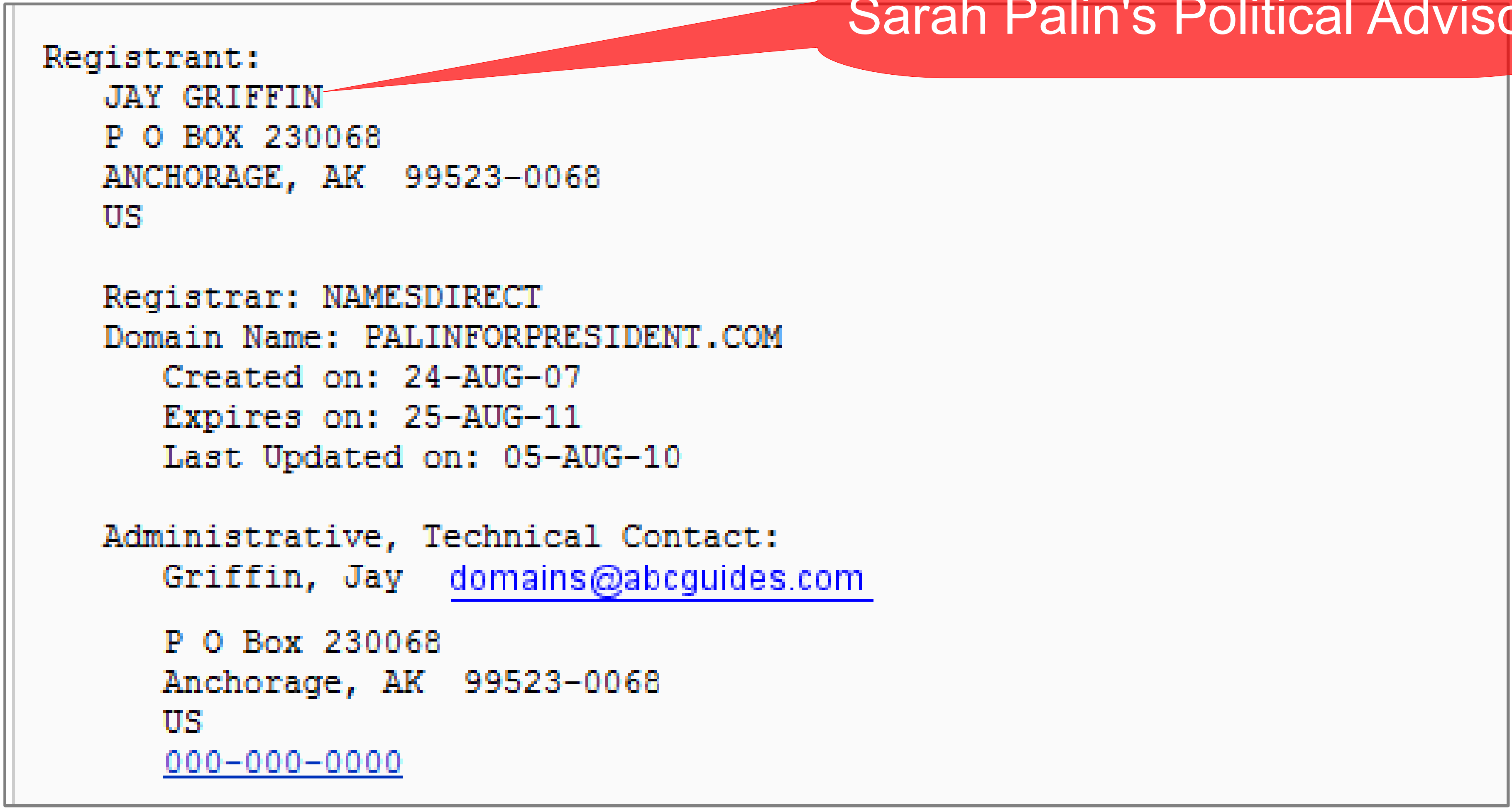
Mar 17, 2014, 4544 domains
Aug 05, 2014, **6411** domains

Monitored DNS records leak historic thinking

At a recent Data Journalism workshop, I asked a group of Investigative Journalists to discover the first documented proof of Sarah Palin's Presidential aspirations.

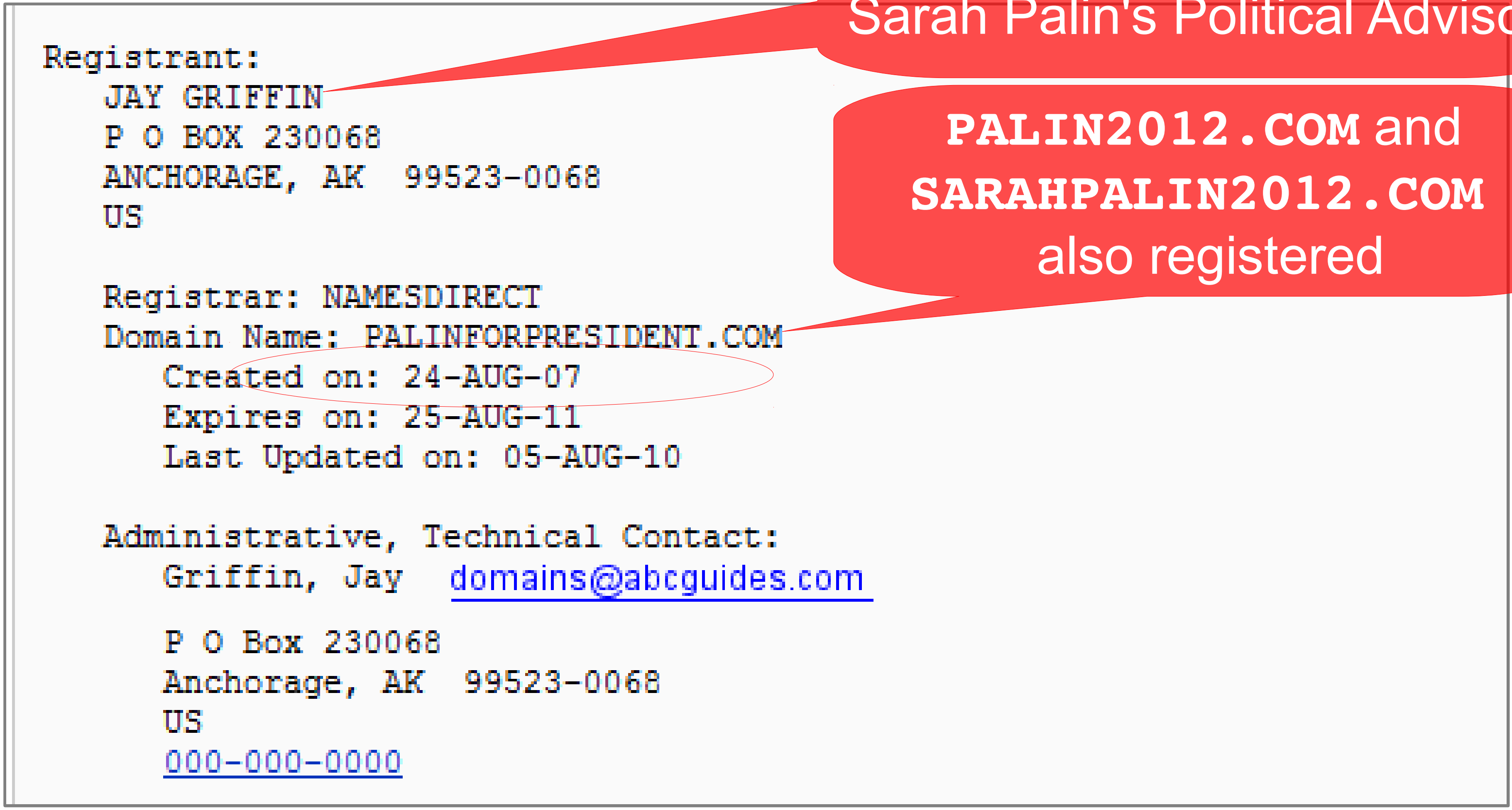
Monitored DNS records leak historic thinking

Jay Griffin was
Sarah Palin's Political Advisor.



```
Registrant:
   JAY GRIFFIN
   P O BOX 230068
   ANCHORAGE, AK  99523-0068
   US

   Registrar: NAMESDIRECT
   Domain Name: PALINFORPRESIDENT.COM
      Created on: 24-AUG-07
      Expires on: 25-AUG-11
      Last Updated on: 05-AUG-10

   Administrative, Technical Contact:
      Griffin, Jay  domains@abcguides.com

      P O Box 230068
      Anchorage, AK  99523-0068
      US
      000-000-0000
```

Monitored DNS records leak historic thinking

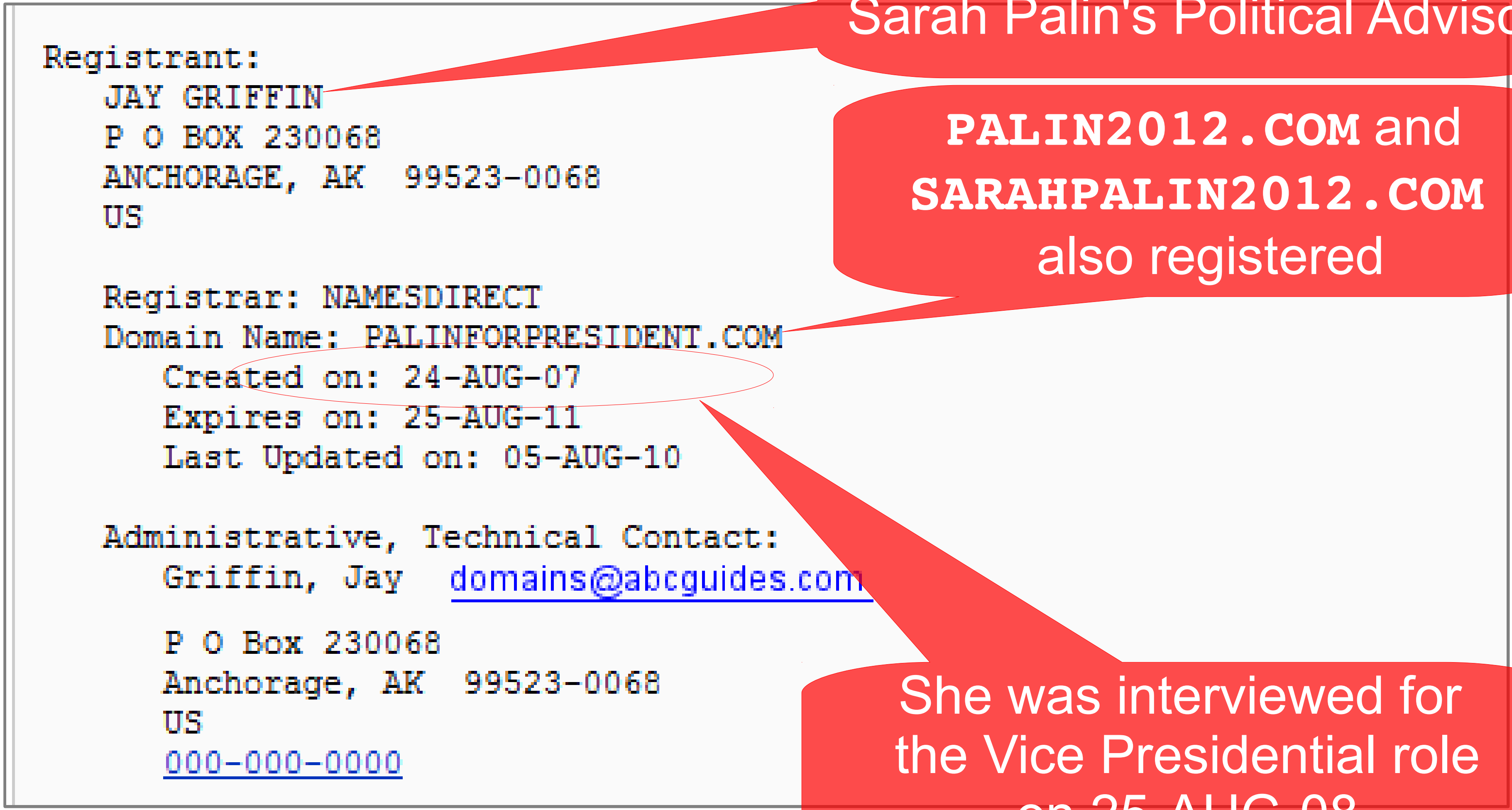


```
Registrant:
   JAY GRIFFIN
   P O BOX 230068
   ANCHORAGE, AK  99523-0068
   US

   Registrar: NAMESDIRECT
   Domain Name: PALINFORPRESIDENT.COM
      Created on: 24-AUG-07
      Expires on: 25-AUG-11
      Last Updated on: 05-AUG-10

   Administrative, Technical Contact:
      Griffin, Jay  domains@abcguides.com

      P O Box 230068
      Anchorage, AK  99523-0068
      US
      000-000-0000
```

Jay Griffin was
Sarah Palin's Political Advisor.

PALIN2012.COM and
SARAHPALIN2012.COM
also registered

Monitored DNS records leak historic thinking



```
Registrant:
   JAY GRIFFIN
   P O BOX 230068
   ANCHORAGE, AK  99523-0068
   US

   Registrar: NAMESDIRECT
   Domain Name: PALINFORPRESIDENT.COM
      Created on: 24-AUG-07
      Expires on: 25-AUG-11
      Last Updated on: 05-AUG-10

   Administrative, Technical Contact:
      Griffin, Jay  domains@abcguides.com

      P O Box 230068
      Anchorage, AK  99523-0068
      US
      000-000-0000
```

Jay Griffin was
Sarah Palin's Political Advisor.

PALIN2012.COM and
SARAHPALIN2012.COM
also registered

She was interviewed for
the Vice Presidential role
on 25-AUG-08

Employees inadvertently leak trade secrets outside of work

What an HR Director thinks

This company is only as great as its employees

To succeed I need to hire, train and retain the best

My employee list is a trade secret

Employees inadvertently leak trade secrets outside of work

What an HR Director thinks

This company is only as great as its employees

To succeed I need to hire, train and retain the best

My employee list is a trade secret

What a hacker thinks

Employees inadvertently leak trade secrets outside of work

What an HR Director thinks

This company is only as great as its employees

To succeed I need to hire, train and retain the best

My employee list is a trade secret

What a hacker thinks

Within minutes I can discover who all your Business Development people are

Employees inadvertently leak trade secrets outside of work

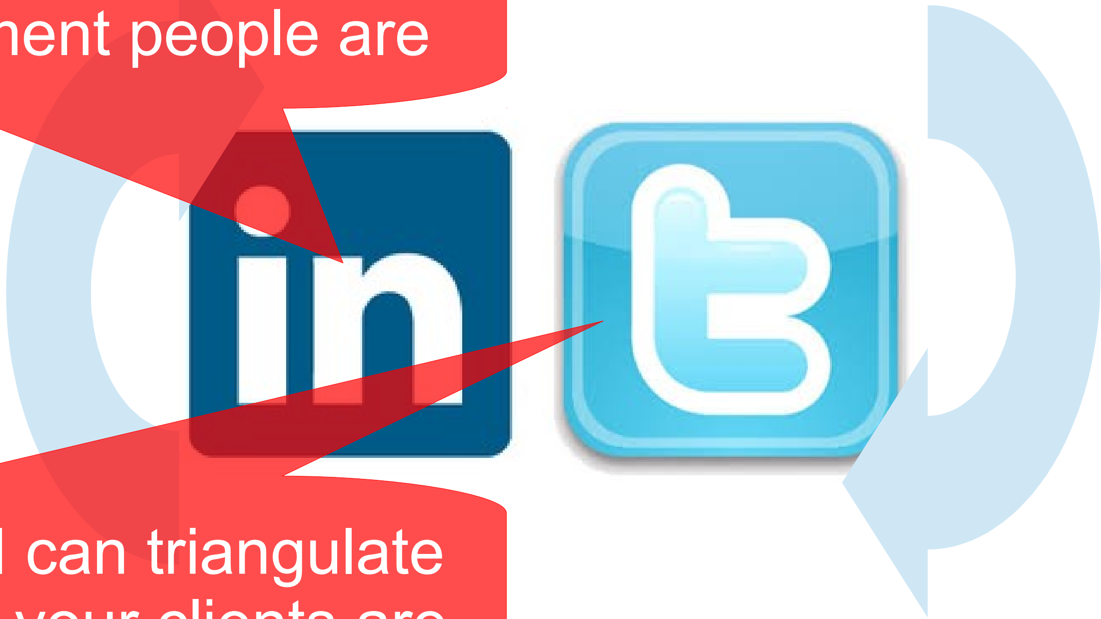
What an HR Director thinks

This company is only as great as its employees

To succeed I need to hire, train and retain the best

My employee list is a trade secret

What a hacker thinks

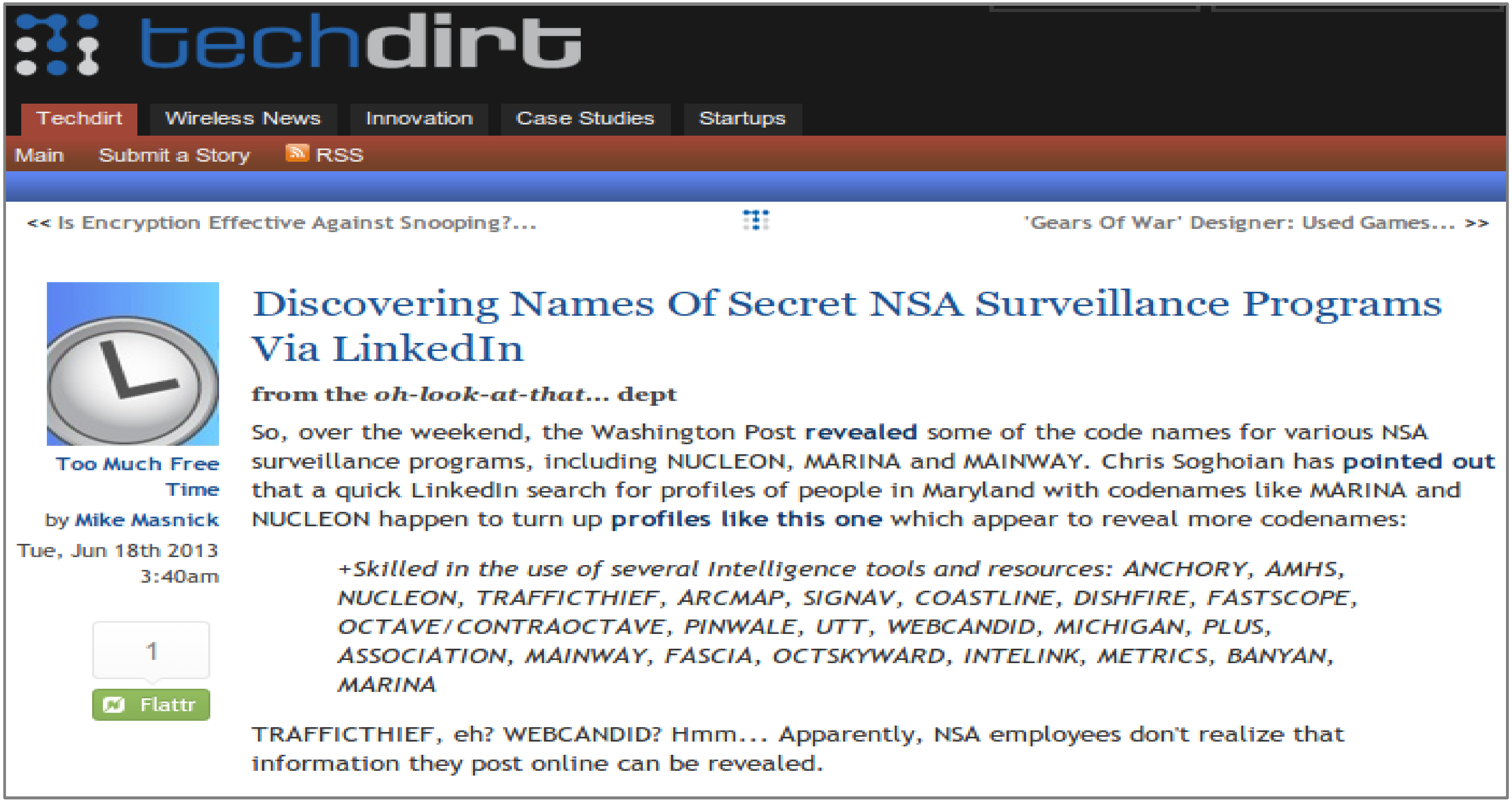


Within minutes I can discover who all your Business Development people are

Within a few more minutes I can triangulate with Twitter to discover who your clients are

You're Leaking Trade Secrets

You can't keep employees from using social media



<< Is Encryption Effective Against Snooping?...

'Gears Of War' Designer: Used Games... >>

Discovering Names Of Secret NSA Surveillance Programs Via LinkedIn

Too Much Free Time

by Mike Masnick

Tue, Jun 18th 2013 3:40am

1

Flattr

from the *oh-look-at-that...* dept

So, over the weekend, the Washington Post **revealed** some of the code names for various NSA surveillance programs, including NUCLEON, MARINA and MAINWAY. Chris Soghoian has **pointed out** that a quick LinkedIn search for profiles of people in Maryland with codenames like MARINA and NUCLEON happen to turn up **profiles like this one** which appear to reveal more codenames:

> *+Skilled in the use of several Intelligence tools and resources: ANCHORY, AMHS, NUCLEON, TRAFFICTHIEF, ARCMAP, SIGNAV, COASTLINE, DISHFIRE, FASTSCOPE, OCTAVE/CONTRAOCTAVE, PINWALE, UTT, WEBCANDID, MICHIGAN, PLUS, ASSOCIATION, MAINWAY, FASCIA, OCTSKYWARD, INTELINK, METRICS, BANYAN, MARINA*

TRAFFICTHIEF, eh? WEBCANDID? Hmm... Apparently, NSA employees don't realize that information they post online can be revealed.

Use corporate social media accounts for marketing, etc.

Social Media accounts
are becoming
Intellectual Property

Recommendations

- You can't avoid many of these leaks
  - Regulatory information
  - Public notices for licensing

Recommendations

- You can't avoid many of these leaks
  - Regulatory information
  - Public notices for licensing
- Be aware that your competition has the same issues

Recommendations

You can't avoid many of these leaks

- Regulatory information
- Public notices for licensing

Be aware that your competition has the same issues

Think about what could happen if your web site is monitored and changes databased

Recommendations

Use DNS registration proxies

Recommendations

Use DNS registration proxies

Don't host your own corporate website

Recommendations

Make people realize that organizational privacy benefits everyone

Recommendations

Make people realize that organizational privacy benefits everyone

Have enforceable policies

Recommendations

Make people realize that organizational privacy benefits everyone

Have enforceable policies

Audit EVERYTHING that you publish

Recommendations

Don't disclose organizational information on every job posting

Recommendations

Don't disclose organizational information on every job posting

Use cookies to track competitors coming to your website

Recommendations

Don't disclose organizational information on every job posting

Use cookies to track competitors coming to your website

Turn your website into a recruiting site when competitors visit.

DEFCON 22

You're Leaking TRADE SECRETS

Thank you