

Security for Managers

Everything you need to know, but were afraid to ask

> whoami



Mario Areias

Developer + **Security**

Security **can** be Agile

Agile **should** be Secure

Security is **not** mentioned
in Agile Manifesto



photo: Christopher Ferguson

Agile Manifesto

Principles behind the Agile Manifesto

Continuous attention to technical excellence and good design enhances agility.

Simplicity--the art of maximizing the amount of work not done--is essential.

Security is a **hard** sell

Everything we **build**
has **Security** implications

What **assets** are you
protecting?



As a user

I want to upload a photo

**So I can share it with my
friends**



As a **user**

I want to **upload** a **photo**

So I can **share** it with my
friends

Security is about **context**



As a **user**

I want to **upload** a **photo**

So I can **share** it with my
friends

What is the **impact** on
your **users** in case of a
data **breach**?

**Security is about
risk management**

The Equifax logo, featuring the word "EQUIFAX" in a white, italicized, sans-serif font on a dark red rectangular background.

data **breach**

Names

148 million

Addresses

SSNs

EQUIFAX

data **breach**



The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

The Equifax logo, featuring the word "EQUIFAX" in a bold, white, italicized sans-serif font, set against a dark red rectangular background.

data breach

A culture of cybersecurity
complacency

The Equifax logo, featuring the word "EQUIFAX" in a bold, white, sans-serif font with a stylized 'Q' that has a tail, set against a dark red rectangular background.

data **breach**



TECH

Equifax just became the first company to have its outlook downgraded for a cyber attack

PUBLISHED WED, MAY 22 2019 • 4:50 PM EDT | UPDATED WED, MAY 22 2019 • 6:47 PM EDT

<https://www.cnbc.com/2019/05/22/moodys-downgrades-equifax-outlook-to-negative-cites-cybersecurity.html>

EQUIFAX

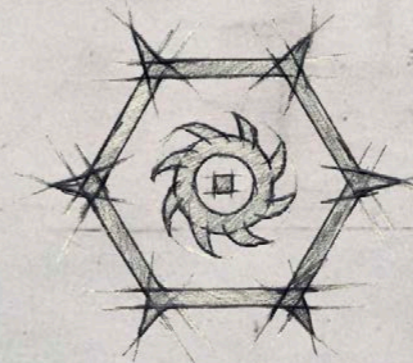
data **breach**




The Equifax Data Breach

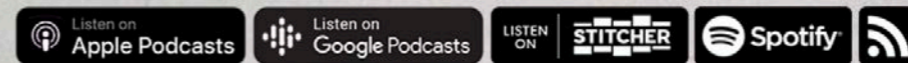
Majority Staff Report
115th Congress

December 2018



MALICIOUSLIFE

by  cybereason



The Equifax Data Breach Pt. I: A Big Data Bubble



data **breach**

Names

139 million

Hashed

Passwords

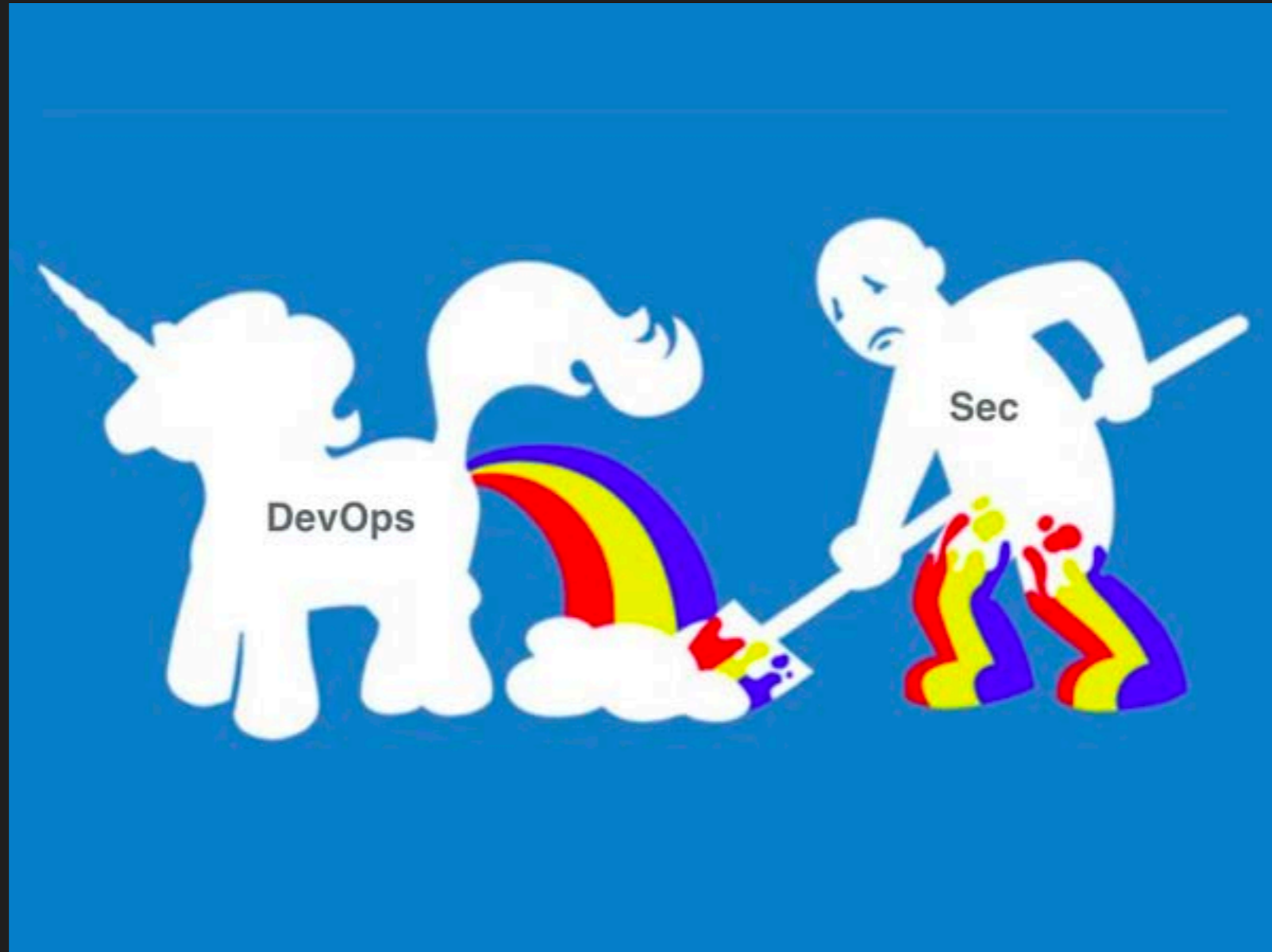
Partial

Payment Info

Is your **organisation**
doing **enough** to
protect its assets?

Security is hard.







DEVSECOPS

<http://www.etsy.com/shop/sharpwriter>

WEUSER 2012
memegenerator.net

What about **managers**?

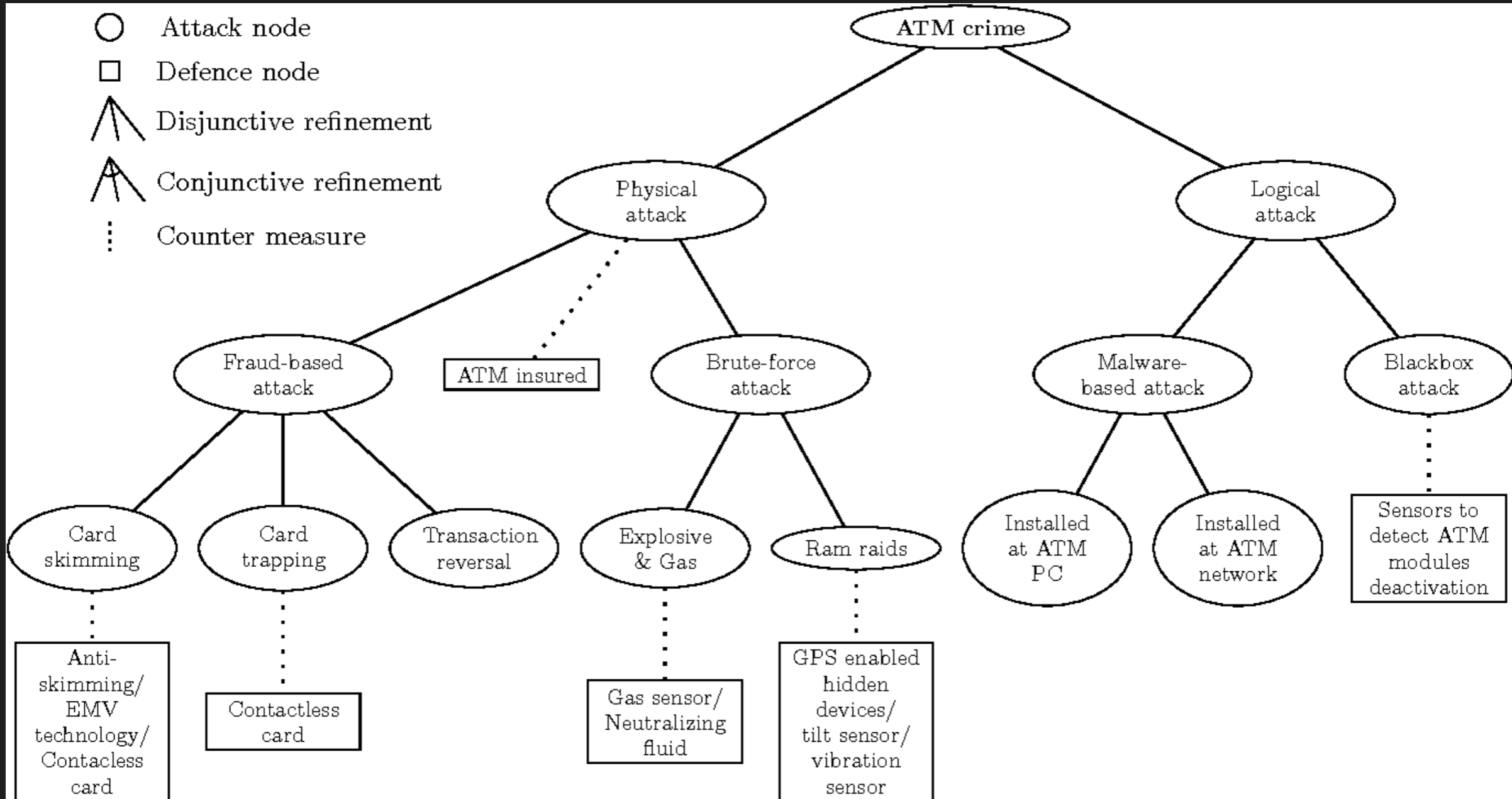
The **basics** can get **you** a
long way

Security **Champions**
As **bridges** between Dev
and Security

**Education as a resource
to prevent basic
security bugs**

Threat Model
Evil User stories

- Attack node
- Defence node
- ⋈ Disjunctive refinement
- ⋂ Conjunctive refinement
- ⋮ Counter measure



Pen test your application
to verify its security
controls

Trust, but **verify** your
vendors and **partners**

Involve, **engage**
Security **early** and often

Security is **everyone's** job

Security **can** be Agile

Agile **should** be Secure

Agile + Security = Velocity

What **assets** are you **protecting**?

What is the **impact** on your **users** in case of a data **breach**?

Is your **organisation** doing **enough** to **protect** its assets?



Thank you!