# Making Security Everyone's Responsibility

James Stewart I@jystewart I james@jystewart.net

Background in software development and product management

Co-founded UK Government Digital Service

Deputy CTO, UK Government

Now independent advisor on digital change, technology and security

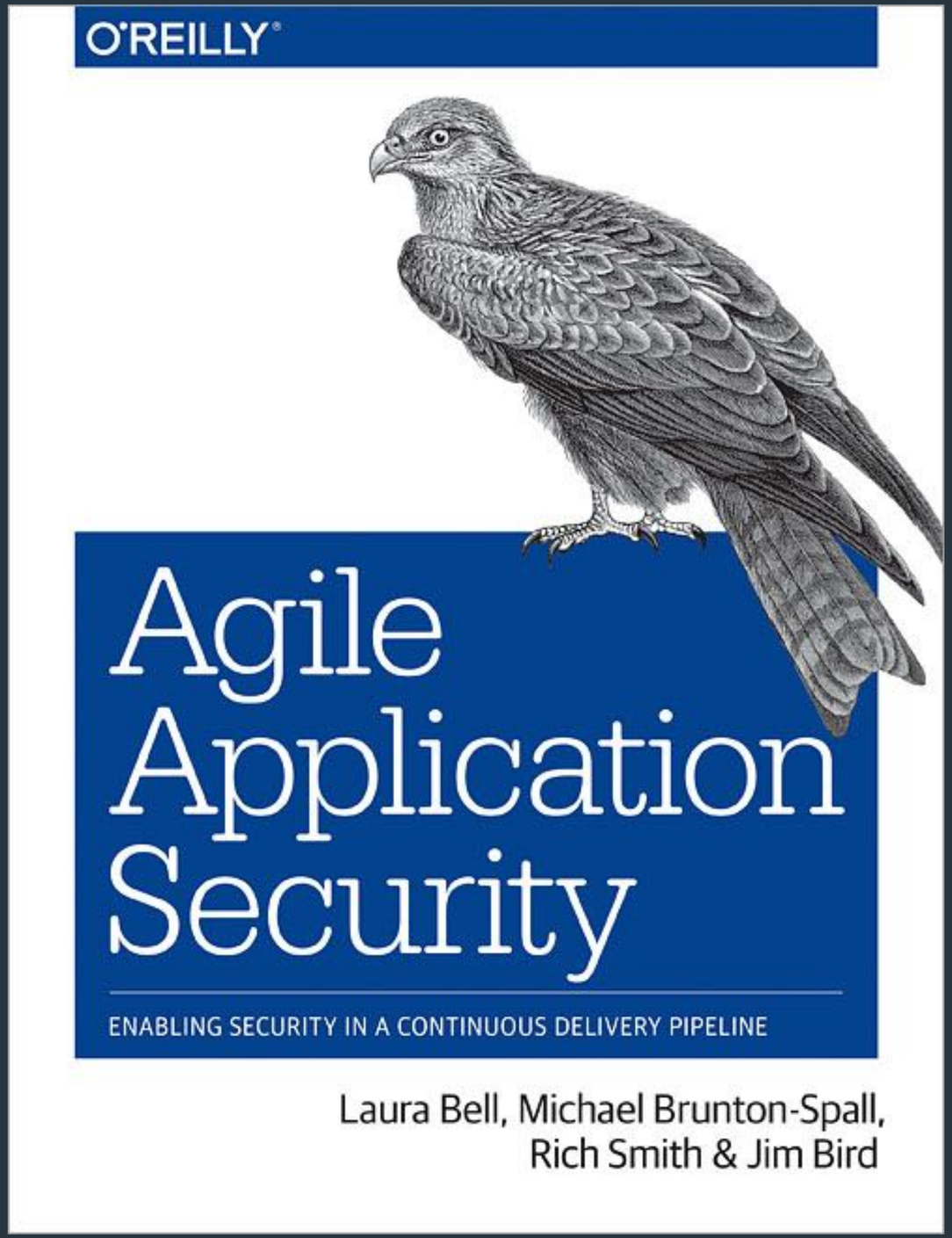
@jystewart | james@jystewart.net

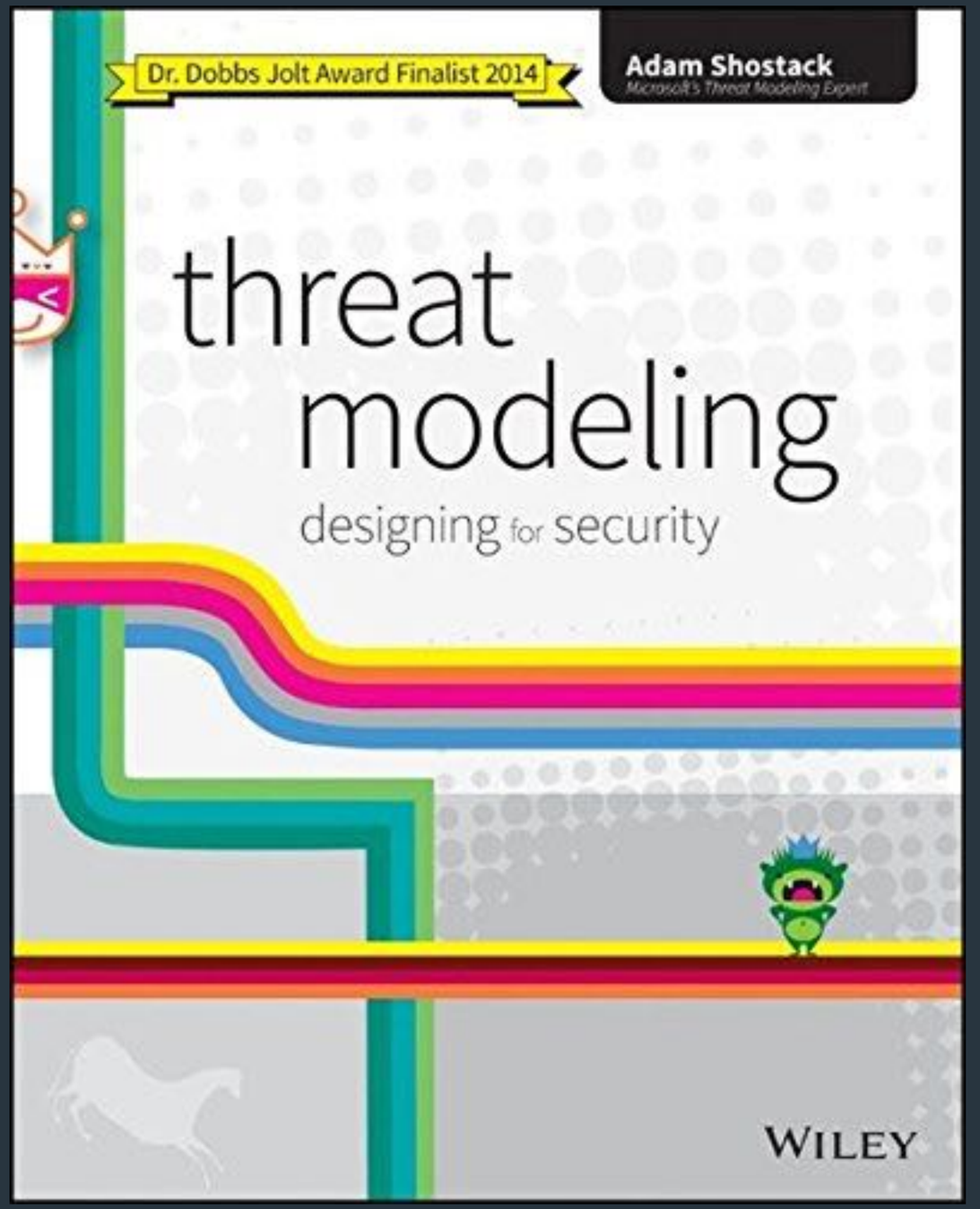
# Context

- new product team struggling with prioritising security
- working with a complex service to become more agile
- moving to a new team and want to leave a clear understanding

# Goals

- ensure security is a cross-disciplinary concern
- build an understanding of the landscape
- develop ways to make this thinking part of agile working
- stimulate a more security-conscious culture


O'REILLY
Agile Application Security
ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE
Laura Bell, Michael Brunton-Spall,
Rich Smith & Jim Bird


Dr. Dobbs Jolt Award Finalist 2014
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY

“Why does everyone who works in government become obsessed with security?”

@jystewart

It’s all about
**trust** and
**competence**

@jystewart

GOV.UK

# Welcome to GOV.UK

The best place to find government services and information
**Simpler, clearer, faster**

Search GOV.UK

Popular on GOV.UK

**Universal Jobmatch job search**

**Renew vehicle tax**

**Benefits**
Includes eligibility, appeals, tax credits and Universal Credit

**Births, deaths, marriages and care**
Parenting, civil partnerships, divorce and Lasting Power of Attorney

**Business and self-employed**
Tools and guidance for businesses

WIKIPEDIA
The Free Encyclopedia

Not logged in Talk Contributions Create account Log in

Article Talk | Read Edit View history | Search Wikipedia

# 2016 Dyn cyberattack

From Wikipedia, the free encyclopedia

Main page
Contents
Featured content
Current events
Random article
Donate to Wikipedia
Wikipedia store

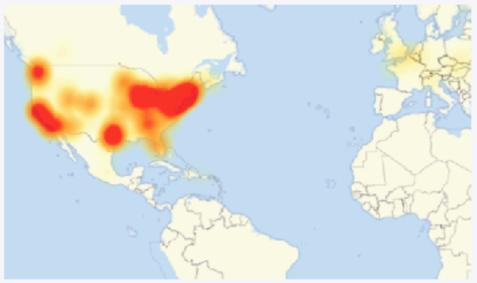
Interaction

Help
About Wikipedia
Community portal
Recent changes

The **2016 Dyn cyberattack** took place on October 21, 2016, and involved multiple distributed denial-of-service attacks (DDoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn, which caused major Internet platforms and services to be unavailable to large swathes of users in Europe and North America.[2][3] The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.[4]

As a DNS provider, Dyn provides to end-users the service of mapping an Internet domain name—when, for instance, entered into a web browser—to its corresponding IP address. The distributed denial-of-service (DDoS) attack was accomplished through a large number of DNS lookup requests from tens

**Dyn cyberattack**



Map of areas most affected by attack, 16:45 UTC, 21 October 2016.[1]

| | |
|---|---|
| **Date** | October 21, 2016 |

https://insidegovuk.blog.gov.uk/2016/11/15/incident-report-gov-uk-dns-outage/

Hacking

# Equifax hack: two executives to lea company after breach

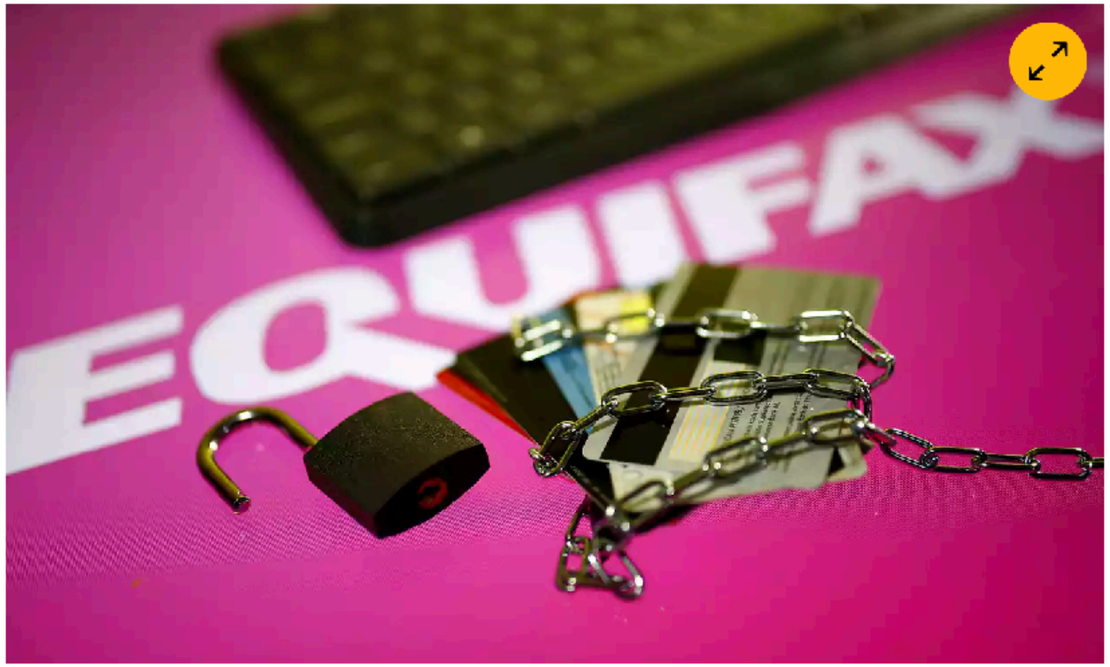
Chief information officer and chief security officer to exit immediately, announces as it highlights security efforts


Equifax announced the departures of two executives. Photograph: Justin Lane/EPA

Hacking

# Equifax hack: credit monitoring company criticized for poor response

Customers and security experts say response to breach that exposed personal data of 143 million Americans has been disorderly and under-resourced




The hack included names, social security numbers, addresses, birthdays and driver's licence numbers. Photograph: Dado Ruvic/Reuters

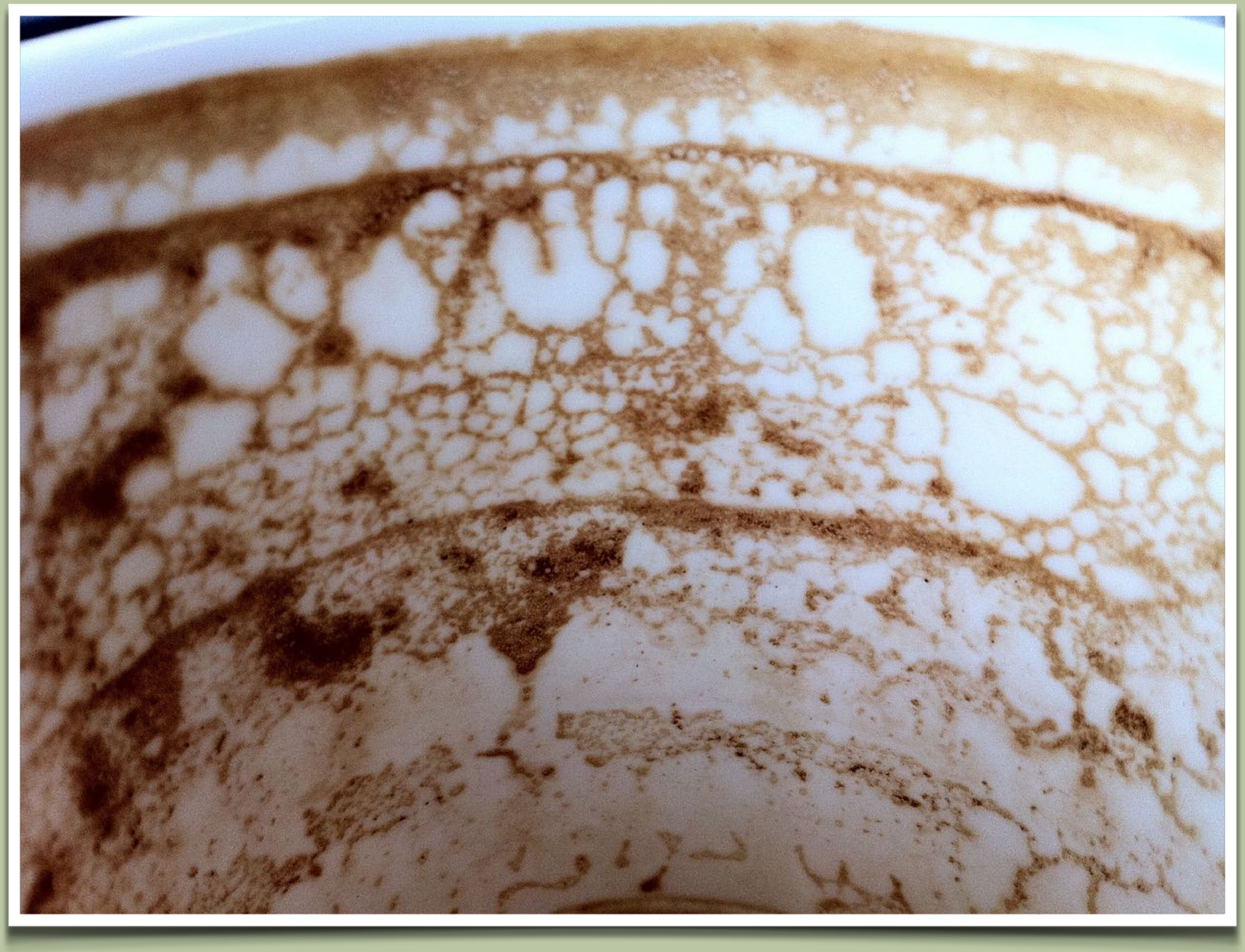
https://www.theguardian.com/technology/2017/sep/08/equifax-hack-credit-social-security-helpline-response-criticism

MAT HONAN GEAR 08.06.12 8:01 PM

# HOW APPLE AND AMAZON SECURITY FLAWS LED TO MY EPIC HACKING

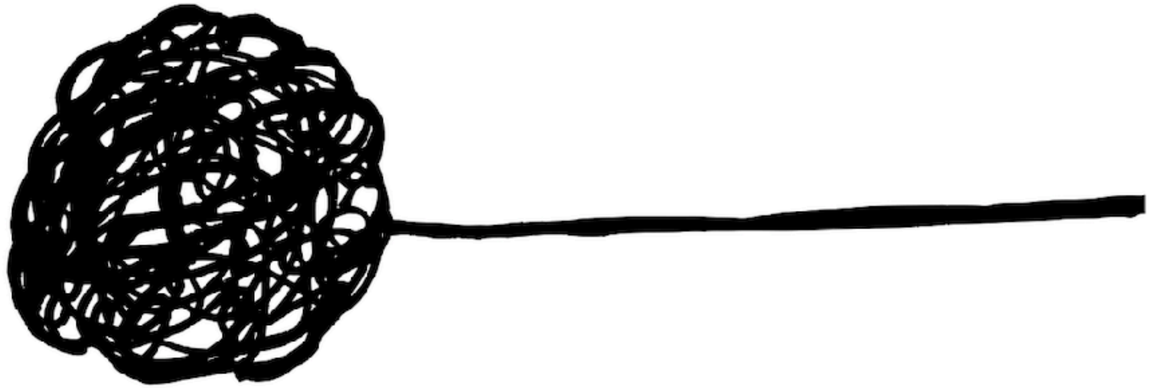
https://www.wired.com/2012/08/apple-amazon-mat-honan-hacking/


https://scotthelme.co.uk/protect-site-from-cryptojacking-csp-sri/



https://flic.kr/p/8Bguco

# Do the hard work to make it simple



Government Digital Service
**Design Principles**

1. Start with needs
2. Do less
3. Design with data
4. Do the hard work to make it simple
5. Iterate. Then iterate again.
6. Build for inclusion
7. Understand context
8. Build digital services, not websites
9. Be consistent, not uniform
10. Make things open: it makes things better

https://www.gov.uk/design-principles & https://www.flickr.com/photos/psd/9104280608/

“

Hackers stole a total of £130bn from consumers in 2017, including £4.6bn from British internet users, according to a new report from cybersecurity firm Norton.

**The most common crimes were generally low-tech**, such as attempts to trick individuals into revealing their personal information through bogus emails with generally low costs to victims.

”

https://www.theguardian.com/technology/2018/jan/23/cybercrime-130bn-stolen-consumers-2017-report-victims-phishing-ransomware-online-hacking

https://us.norton.com/cyber-security-insights-2017

“Cyber security is not just about technology.

**Almost all successful cyber attacks have a contributing human factor.**”

UK National Cyber Security Strategy

As things move faster, we need new approaches to keep up

We need to provide clear ownership and the ability to change safely

We need to recognise that every system involves humans, not just tech

# We need to apply design thinking

Organisational change is ignited by committed, curious teams

Curious teams are diverse, welcoming and respectful of expertise

# Contents

- techniques to structure our awareness
- activities to engage the wider team
- ways to operationalise this
- what that means for culture

# Definitions

# Threat

“Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Threat

## Something that could go wrong, causing a problem

“Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Impact

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Impact

## How severe are the results?

The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Risk

“The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Risk

## How seriously do we have to take this?

“The level of impact on organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Vulnerability

“A weakness in a system, application, or network that is subject to exploitation or misuse.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Vulnerability
## How might it happen?

“A weakness in a system, application, or network that is subject to exploitation or misuse.”

http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

# Attacker

## Who might do this to us?

# Threat actor

**“People, organisations or entities that might pose a risk to your systems, organisations, and people”**

**- Agile Application Security**

# Confidentiality
# Integrity
# Availability

# Prevention
# Detection
# Recovery

# But what is security?

# Over to you

Get into pairs.

Introduce yourselves, where you work and what you do

Imagine you're making a case for a new team to focus on security. Your product owner asks "what do you mean by security?".

What's your 45 second answer?

Most of the time, security is putting in place the right controls to protect the correct operation of our services and to maintain confidentiality, availability and integrity of information.

Most of the time, security is putting in place the right controls to **protect the correct operation** of our services and to maintain confidentiality, availability and integrity of information.

Another perspective is that it’s an aspect of quality, linked to your core purpose.

And that perhaps “security” isn’t where we should start.

- What do you want to protect?
- Who do you want to protect it from?
- How likely is it that you will need to protect it?
- How bad are the consequences if you fail?
- How much trouble are you willing to go through in order to try to prevent those?

https://motherboard.vice.com/en_us/article/d3devm/motherboard-guide-to-not-getting-hacked-online-safety-guide


# Understanding your risk appetite

What do we **really value**?

What could really **take us out of business**?

The process will depend on how clear your organisation is

# Risk Appetite

**Purpose**
Sets context and frames the conversation.

**Who is it for?**
Senior audience.

**What are the challenges?**
Focusing it down. Expectation management. Getting attention. Broad/ diverse thinking.

**Who should be involved?**
Product/service owner, team leads. Open review process.

# Over to you

Omnivore Direct is an online grocery retailer. They:

- provide a website where you can order your weekly groceries, make your payments, and select a delivery time.
- run a warehouse where food is stored and packed
- have a fleet of vans and are responsible for deliveries

Get into groups and develop a set of objectives. We shouldn’t have more than 5.

Objectives

1. build and maintain our users' trust in our ability to manage their data responsibly
2. minimise losses associated with goods not reaching the intended recipient
3. ensure high level integrity in our supply chain data so we can maintain quality
4. maintain compliance with relevant regulations, e.g. PCI-DSS

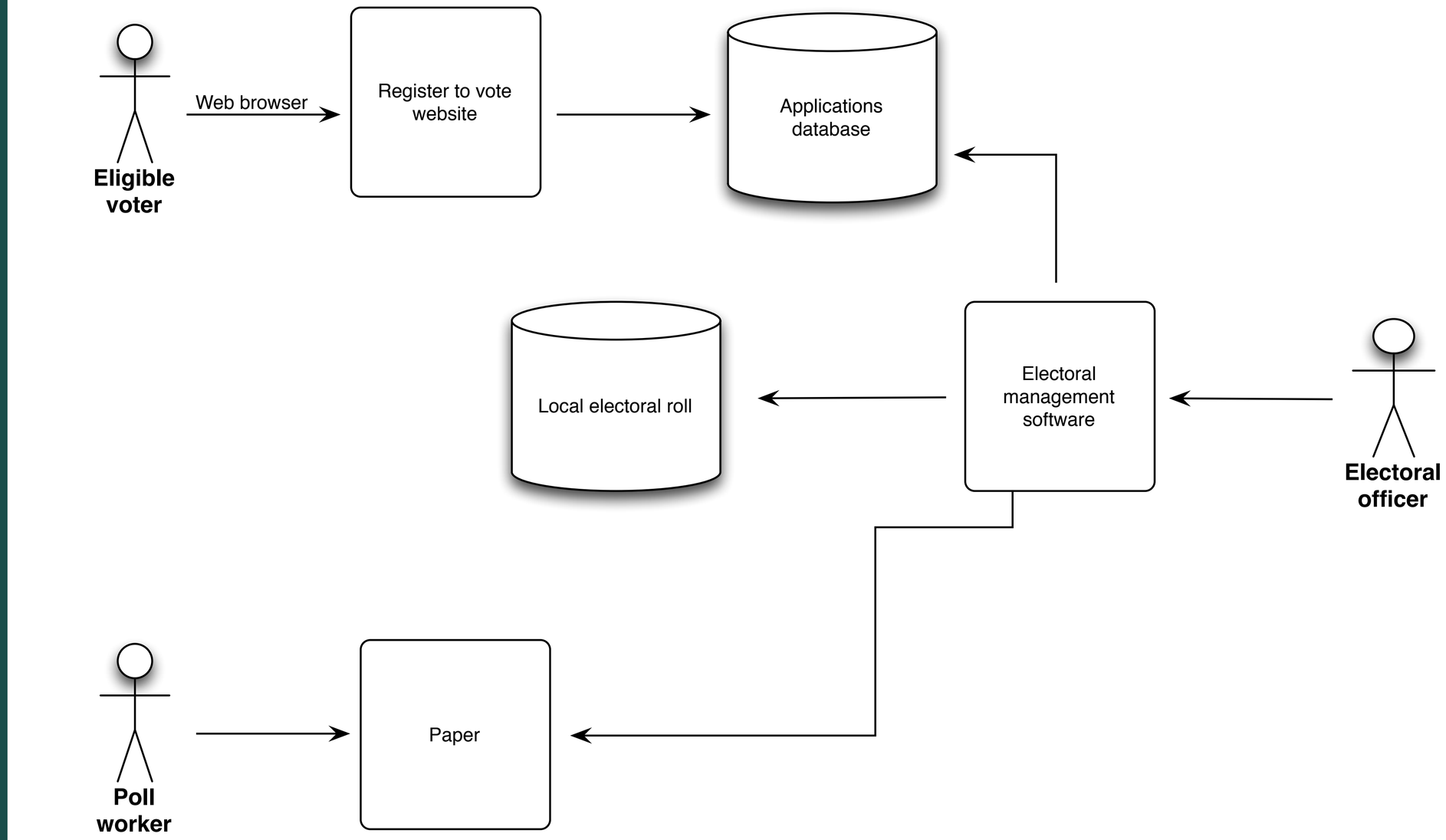
Primary risks:

- Bulk leak of data
- Loss of data integrity
- Loss of availability

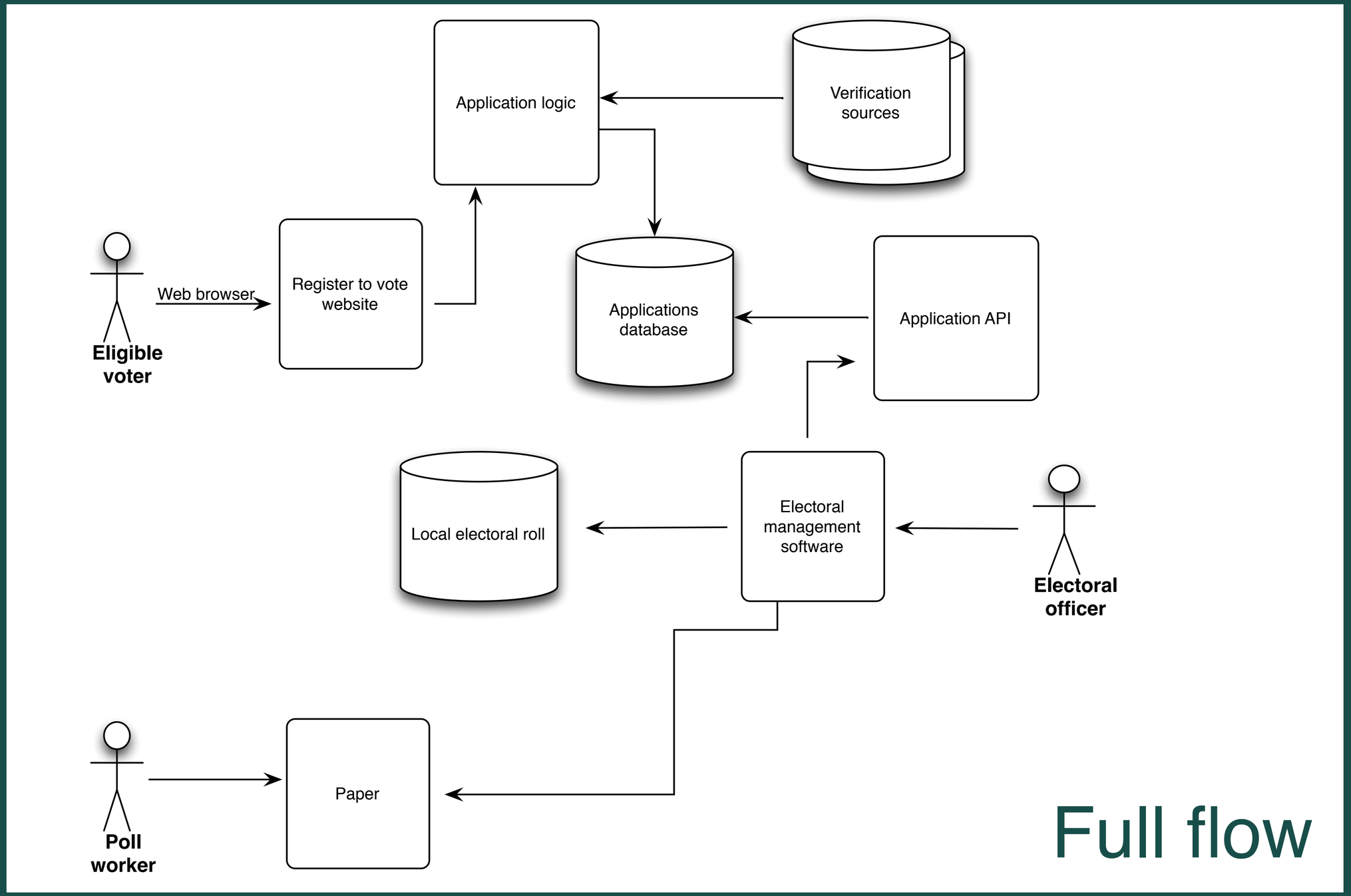
https://docs.google.com/document/d/1QZ05RiD4-0JjnusY79EtWiijyqJbDGruL06OPk-K6sQ/edit


https://flic.kr/p/ppapcZ

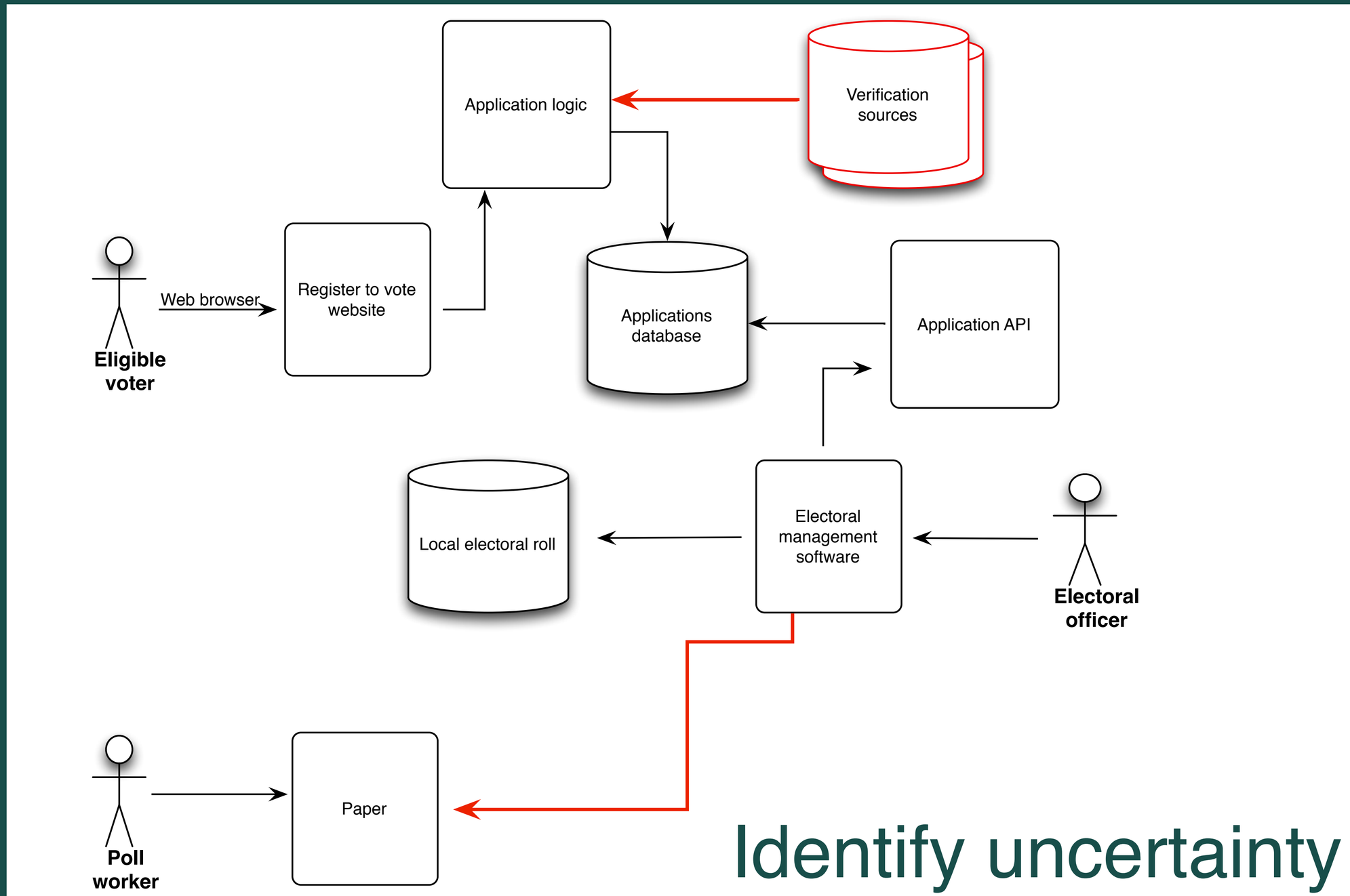
# This is an architecture conference.


Eligible voter
Web browser
Register to vote website
Applications database
Local electoral roll
Electoral management software
Electoral officer
Poll worker
Paper

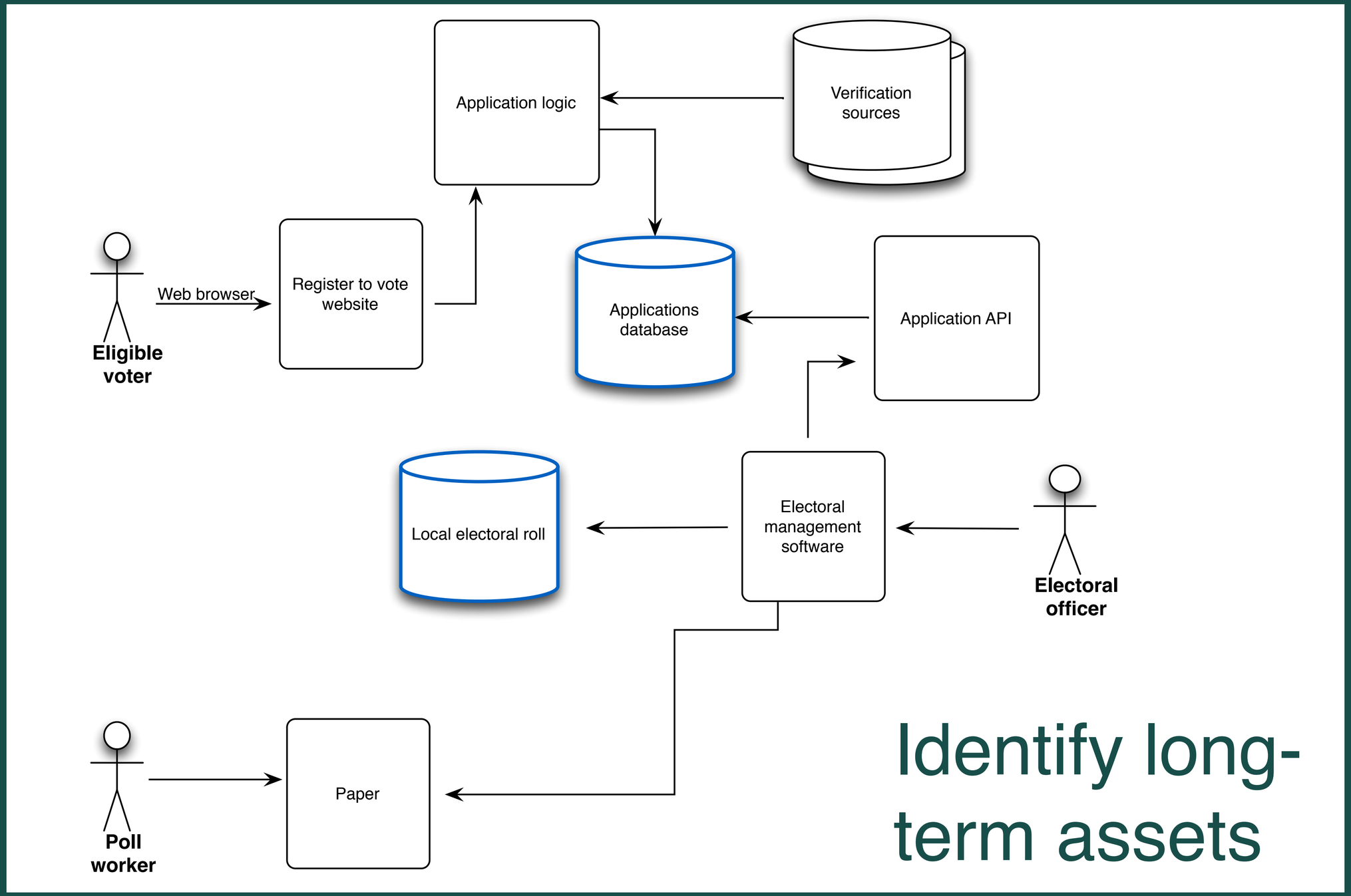
# A first pass


Application logic
Verification sources
Eligible voter
Web browser
Register to vote website
Applications database
Application API
Local electoral roll
Electoral management software
Electoral officer
Poll worker
Paper

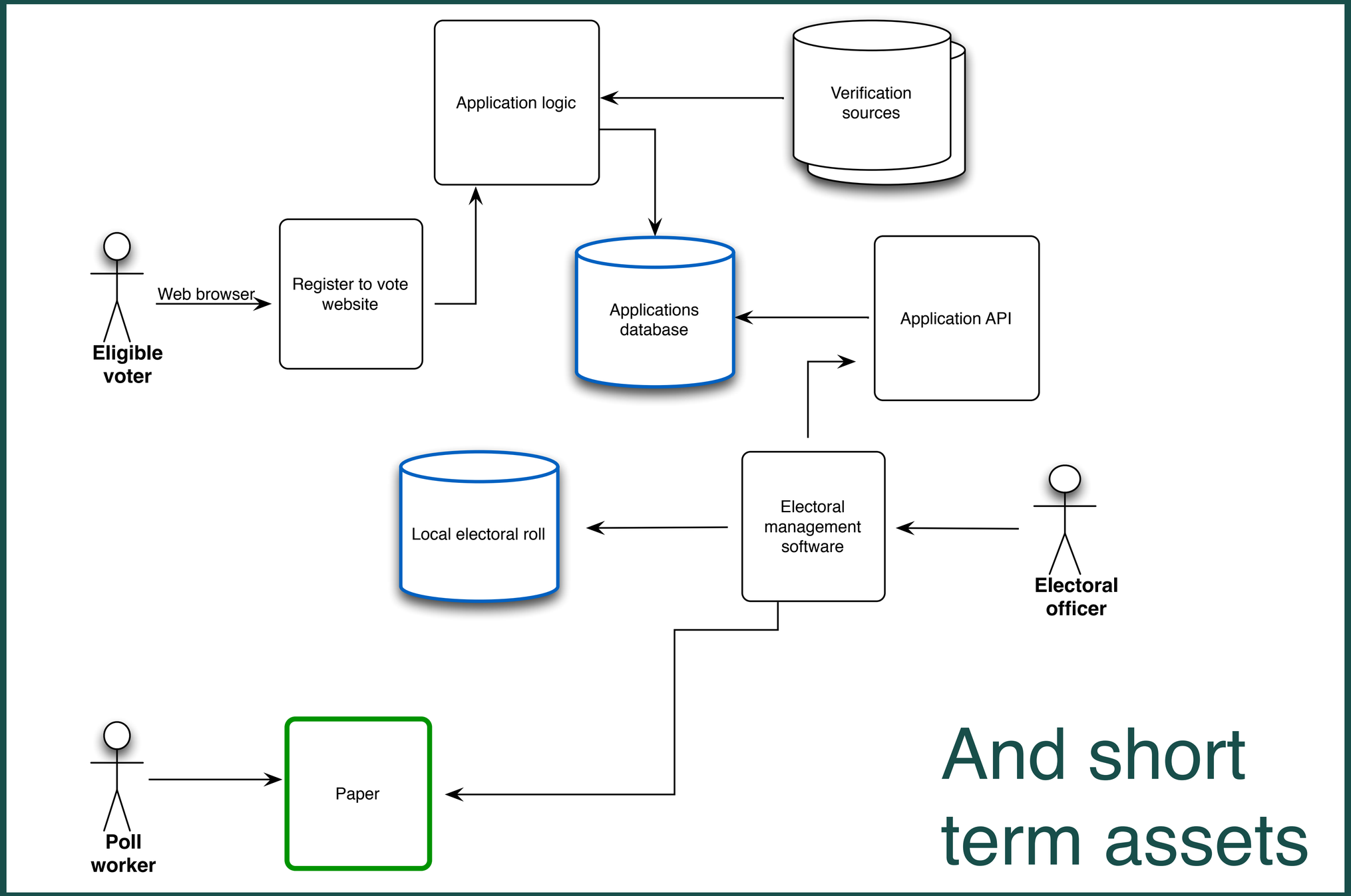
# Full flow



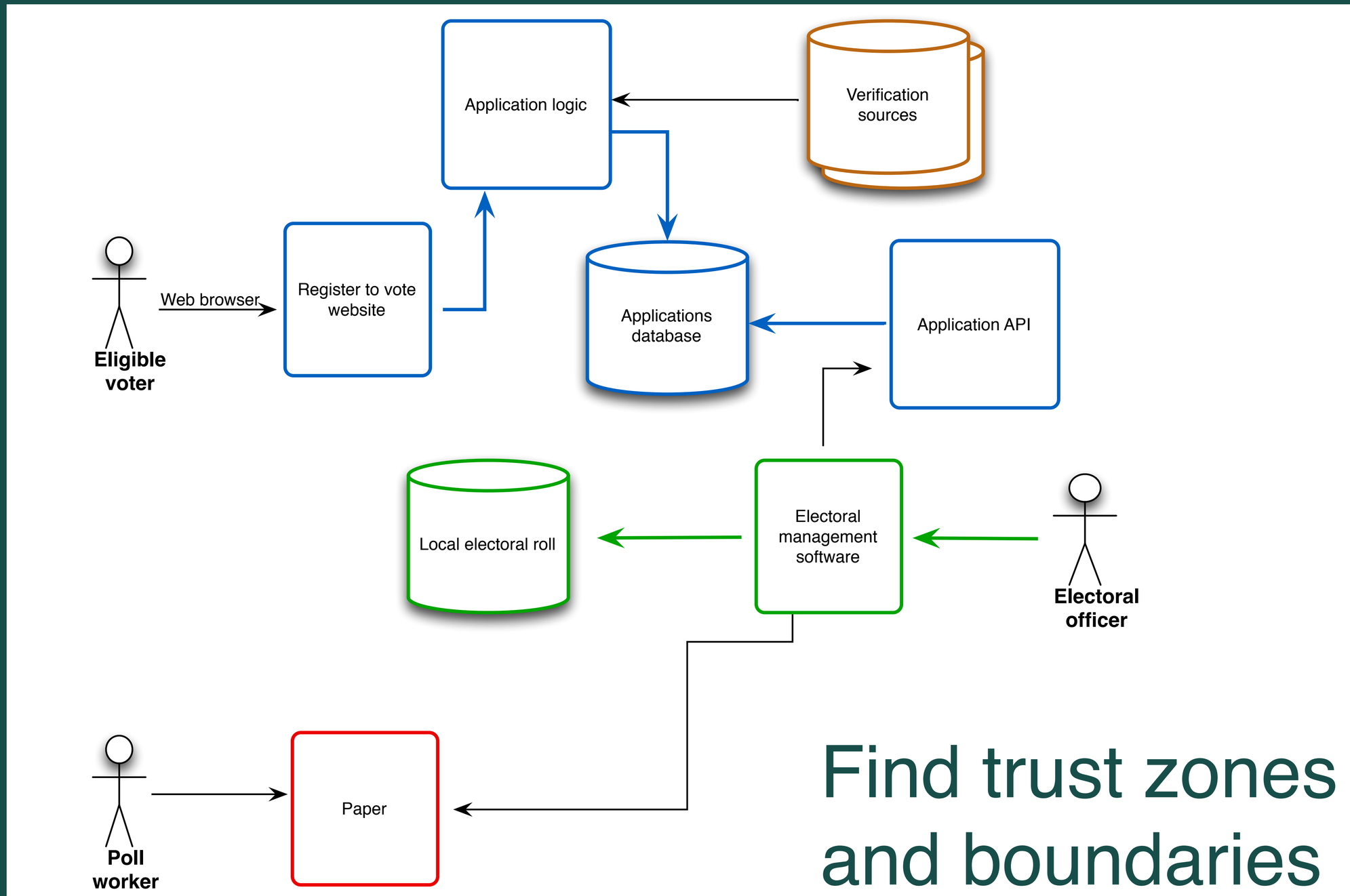

# Identify uncertainty




# Identify long-term assets




# And short term assets




# Find trust zones and boundaries

# Service diagrams

**Purpose**
Ensure you understand the edges of your service across channels

**Who is it for?**
The team and their collaborators

**What are the challenges?**
Making it clear. Setting the boundaries.

**Who should be involved?**
Start in a small group. Invite people in from across the business. Build up iteratively.

“As the information risk owner on GCHQ’s board, in 2014 I was dismayed by a DDoS attack on our website which took it down for a few hours. But in some respects it helped us communicate our strategy. It is a small website of static, basic information about what we do. It is not strategically important in the operational sense and it contains no personal data about anyone. To defend it to the same degree as we defend our state secrets would be an indefensible use of taxpayers’ money. That is risk management in action. Know yourselves, know where your data is right up to the border, and defend accordingly.”

Ciaran Martin, CEO UK National Cyber Security Centre

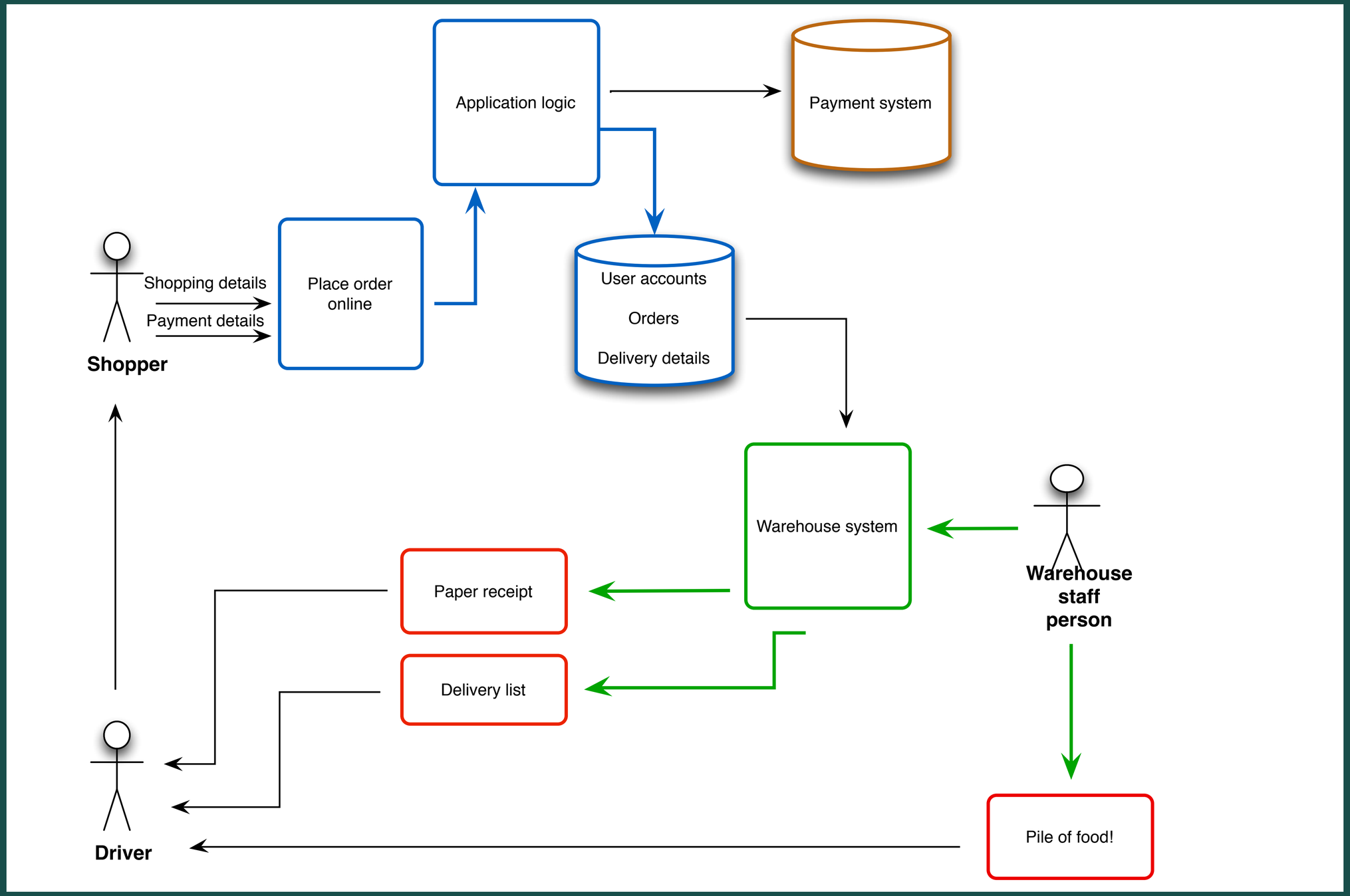
# Over to you

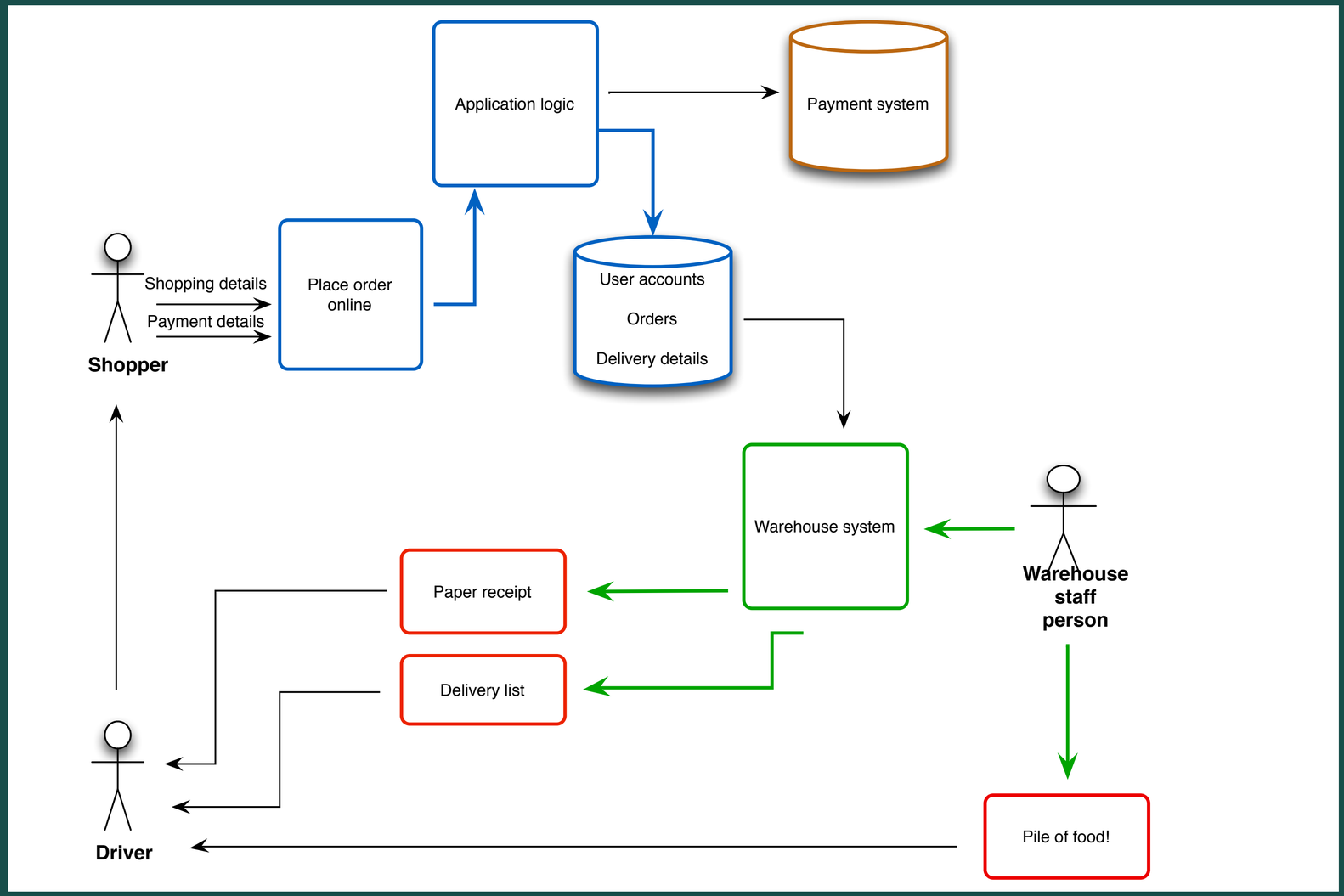
Pick a service you're responsible for, or use…

Omnivore Direct is an online grocery retailer. They:

- provide a website where you can order your weekly groceries, make your payments, and select a delivery time.
- run a warehouse where food is stored and packed
- have a fleet of vans and are responsible for deliveries

Sketch a map of the main parts of the service, and the interactions between them. Identify the main assets and where trust boundaries might be.


Application logic
Payment system
Shopping details
Payment details
Place order online
Shopper
User accounts
Orders
Delivery details
Warehouse system
Warehouse staff person
Paper receipt
Delivery list
Driver
Pile of food!




How do I:

- Reschedule?
- Report problems?
- Change delivery address?


https://flic.kr/p/ppapcZ

It’s important to think about the different groups of people who might attack you

We use terms like “state-sponsored”, “organised crime”, “hacktivists”, “insiders” or “script kiddies”

We can distinguish their motivation, resources and access

# Over to you

Think about the service you've just drawn.

Take a piece of paper list these kinds of threat actors, and see if for each one you can think of something they might want to achieve by attacking your service.

Try and take a view of how important that might be to them, and how much they might be able to invest in it.

| Actor | Goal | Motivation | Investment |
| --- | --- | --- | --- |
| **Insider** | Steal food | Underpaid | ? |
| **State level actor** | Ability to disrupt food supply to an area | Undermine confidence in local government | May be prepared for long term effort including research employees and mapping your systems |
| **Hacktivist** | Change your product catalogue to remove all fruit | Belief that eating fruit is wrong | ? |
| **Organised crime** | Extract order information | Build profile of people for later stings | ? |
| **Script kiddies** | Change everyone's orders | Amusement | Low |

It’s very common to obsess over certain threat actors

We need a way to ground our conversations

# “Personas are models … they get the team on the same page”

Jeff Gothelf
https://www.safaribooksonline.com/library/view/lean-ux-designing/9781491983690

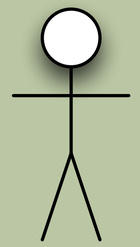
Here are some examples of simple anti-personas:

- Brian is a semiprofessional fraudster
  - — He looks for a return on investment of attacks of at least £10k
  - — Brian doesn't want to get caught, and won't do anything that he believes will leave a trail
  - — Brian has access to simple hacking tools but has little computer experience and cannot write code on his own
- Laura is a low-income claimant
  - — Laura doesn't consider lying to the welfare system immoral and wants to claim the maximum she can get away with
  - — Laura has friends who are experts in the benefits system
  - — Laura has no technical competence
- Greg is an amateur hacker in an online hacking group
  - — Greg wants to deface the site or otherwise leave a calling card
  - — Greg is after defacing as many sites as possible and seeks the easiest challenges
  - — Greg has no financial acumen and is unaware of how to exploit security holes for profit
  - — Greg is a reasonable programmer and is able to script and modify off-the-shelf tools

**From "Agile Application Security"**
**by Laura Bell, Michael Brunton-Spall, Rich Smith, Jim Bird**

Anti-persona

# Brian



**Semi-professional fraudster**

Brian is an opportunist. He doesn't have any real relationship with our organisation but has no qualms about defrauding us.

He does significant research before picking a target and will notice a clear security policy, well configured web servers, and so on.

**This is all conjecture!**

### Motivation

• Looking for a financial return
- Wants a return on investment of at least £10k

### Resources

- Access to simple hacking tools
- No specialist coding or social engineering skills
- Can invest up to £10k providing he will see a return of at least 10x

### Access

• Doesn't know anyone within the company
• Is based a long way from the company's offices
• Has access to a distributed set of servers around the world from which to run attacks

### Disincentives

• Doesn't want to get caught
• Will avoid anything that seems to leave a trail

# Over to you

Look at the work we just did on threat actors.

Take one or two of them and turn them into personas as we've done here.

Begin to think about who in your organisation could help you validate what you have in here.

- Put them somewhere visible
- Review with outside experts
- Continually challenge them
- Seek out threat intelligence

# Anti-personas

**Purpose**
Build common understanding and reference points for prioritisation and testing

**Who is it for?**
The core team

**What are the challenges?**
Getting enough insight

**Who should be involved?**
Try to get an expert in early. Product owner, user

- http://www.cert.org/incident-management/national-csirts/national-csirts.cfm
- https://www.alienvault.com/open-threat-exchange
- https://developers.facebook.com/products/threat-exchange

# Attacks and abuse

https://flic.kr/p/xDzBDT

We hear a lot about phishing, DDOS, social engineering

There are a lot of types of attack, and no widely agreed grouping

There’s also a strong technical bias in how they’re talked about

1. Injection
2. Broken authentication and session management
3. Cross-site scripting (XSS)
4. Insecure direct object references
5. Security misconfiguration
6. Sensitive data exposure
7. Missing function level access control
8. Cross-site request forgery
9. Using components with known vulnerabilities
10. Unvalidated redirects and forwards

https://www.owasp.org/index.php/Top_10_2013-Top_10

- application layer attack
- brute force attack
- distributed denial of service (DDoS) attack
- known vulnerability exploitation
- network protocol attack
- phishing for credentials
- phishing with malware
- rogue update attack
- watering hole attack
- zero day exploitation

https://www.ncsc.gov.uk/document/threat-intelligence-case-studies-cyber-attack-types

- Phishing
- Watering hole
- Whaling attack
- Pretexting
- Baiting and Quid Pro Quo attacks
- Tailgating

http://resources.infosecinstitute.com/common-social-engineering-attacks/

We could go on…
network attacks,
eavesdropping
techniques, etc.

- Spoofing of user identity
- Tampering
- Repudiation
- Information disclosure (privacy breach or data leak)
- Denial of service (D.o.S)
- Elevation of privilege

https://en.wikipedia.org/wiki/STRIDE_(security)

As a (role) I want (something) so that (benefit).

We believe that if we (do thing),
(result will happen)
We'll know we have succeeded when
(something measurable occurs).

- What security guarantees do your users need?
- What mistakes could cause adverse side-effects?
- What might our threat actors want our system to allow?

As threat actor **Greg** I want to **change the delivery address** ***without verifying my identity*** so that I can **get free food.**

# This is done when…

- A reasonable level of identity verification is needed to change delivery address
- This is true across all channels
- The fact of verification is recorded consistently across channels
- We are able to measure the impact on our users

As threat actor Greg I believe that a simple scan using ‘(off the shelf tool here)’ will reveal open routes of access into the system.

# This is done when…

- We have tested with the tool and falsified the assertion
- We are able to repeat this tool regularly using automation
- We know how we would keep track of the availability of other similar tools

# Anti-user stories

**Purpose**
Clearly state what you need to consider, alongside the positive work you need to do. Give you testable outcomes.

**Who is it for?**
The product owner (to prioritise), the team (to understand & implement)

**What are the challenges?**
Not sounding too arbitrary!

**Who should be involved?**
Risk advisors, product owners, everyone in the team.

# Over to you

Take your models, your threat actor personas and (if you like it) the STRIDE model.

Spend a few minutes sketching out some stories, including:

- One positive story where there’s a security guarantee you want to offer to users
- One negative story where there’s something an attacker will want
- Something that will have an impact on operations, not just design and development

For each one, don’t come up with solutions but think about “acceptance criteria”.

Using stories lets us be clear about users, intent, and trade-offs

# Risks and defence

https://flic.kr/p/6q7reN

“Most security practices are about preventing bad things from happening to your information or systems. But risk calculation isn’t about stopping things, it’s about understanding what could happen and how so that you can prioritise your improvements.”

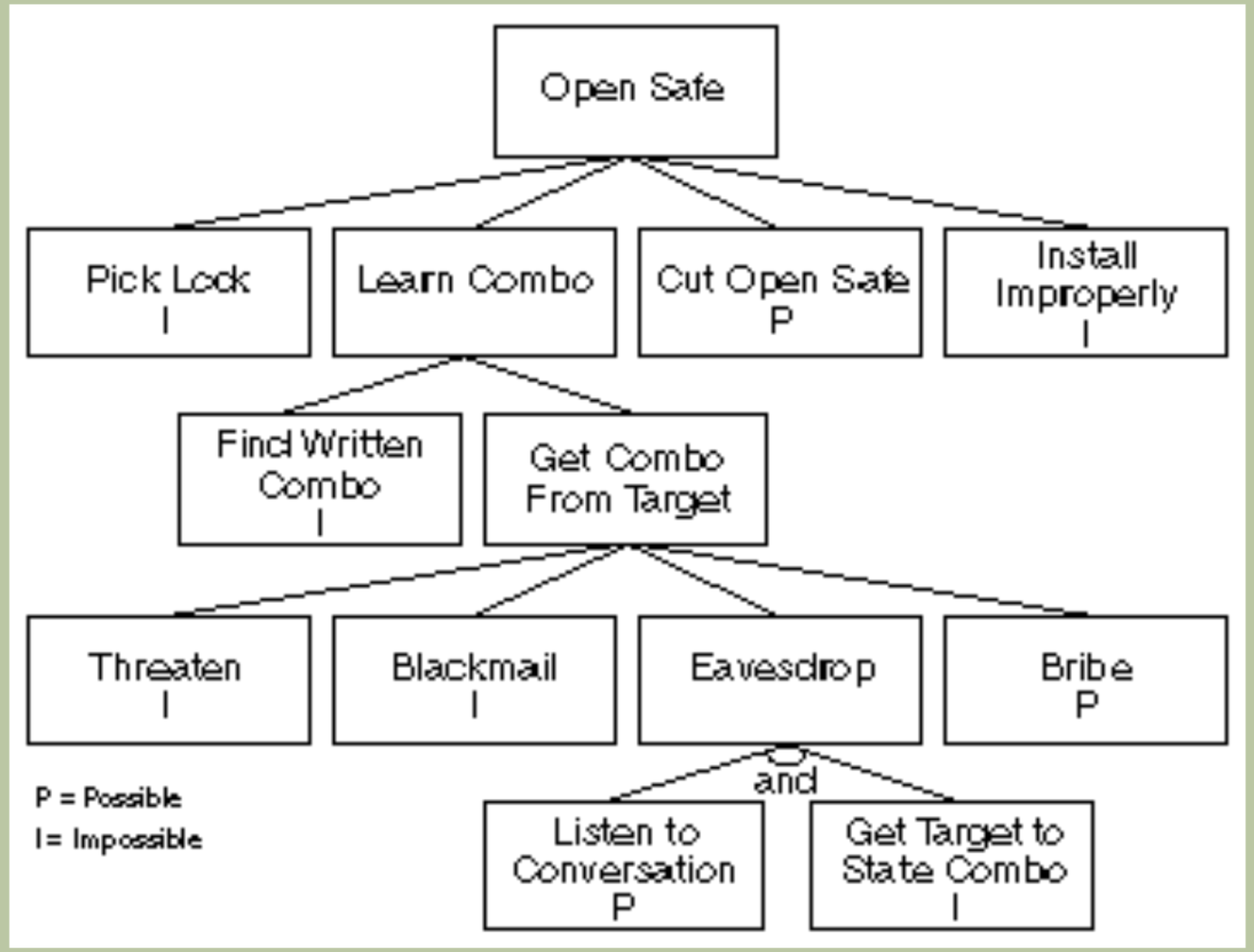
Ciaran Martin, CEO of UK National Cyber Security Centre
https://www.ncsc.gov.uk/news/defending-borders-your-business-digital-era

# Security work is full of trade-offs

Design commonly involves a lot of guess work

Understand systems,
own trade-offs,
practice failure.

@jystewart

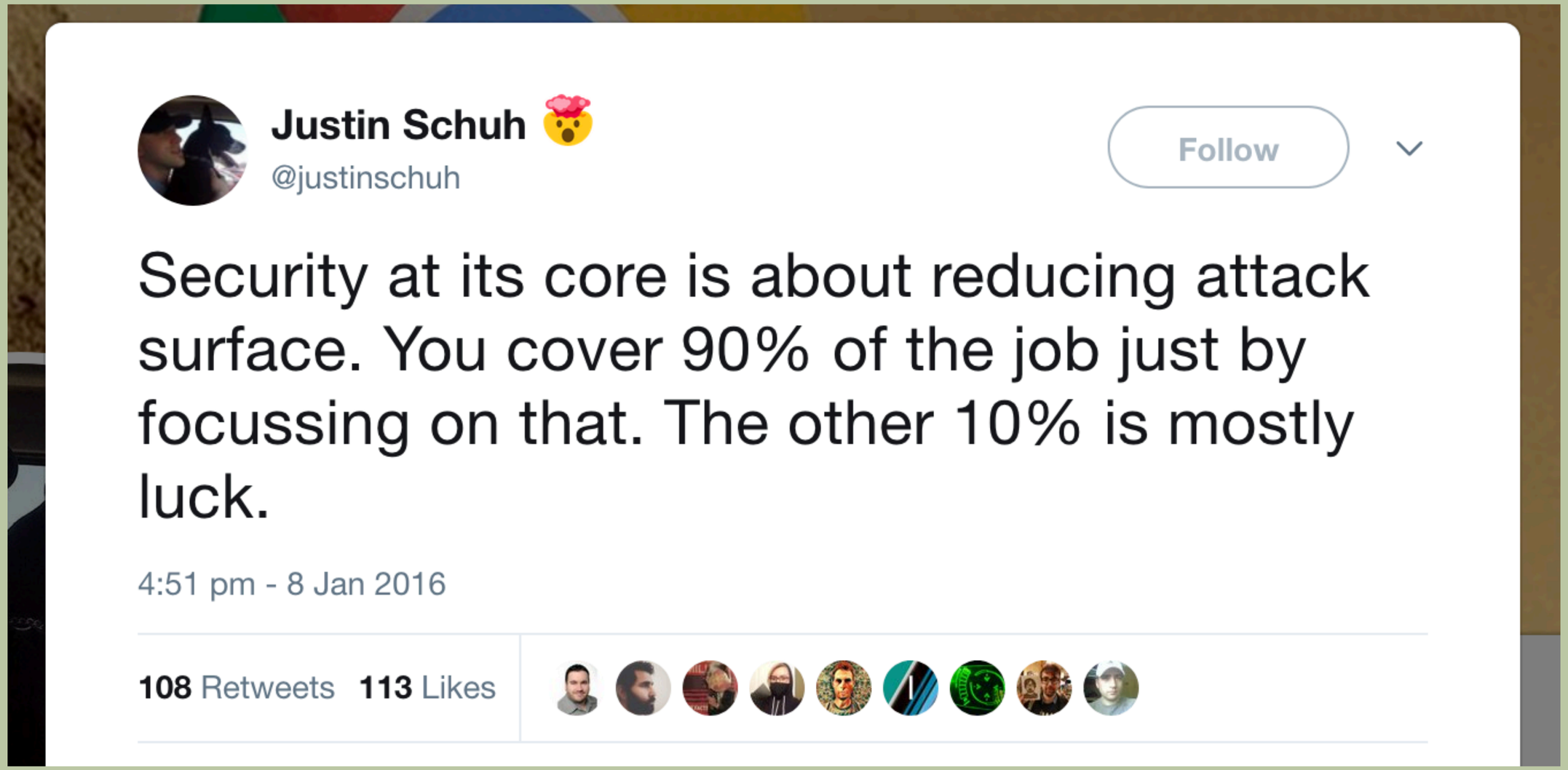



https://www.schneier.com/academic/archives/1999/12/attack_trees.html

# Don’t forget to cover “the basics”

When given the choice, always choose to simplify

@jystewart




https://twitter.com/justinschuh/status/685624978780246016

As threat actor **Greg** I want to **change the delivery address without verifying my identity** so that I can **get free food.**

What does the user need?

- Immediate reassurance?
- List of options?
- Human assistance?

- Provide it all online, re-use login system
- Ask for password when making phone call
- Ask for some private information
- Verify incoming phone number
- Generate a time-limited code online and then ask for it offline

# Over to you

Take one of your stories from the last exercise (or a new one).

Think about the design challenges involved in it

# SECURITY OPERATIONS


# What’s next?

https://flic.kr/p/L1hJFy

Understand systems,
own trade-offs,
practice failure.

@jystewart

# 1. Run through these exercises in diverse groups

# Proactively involve people who don’t expect to be consulted

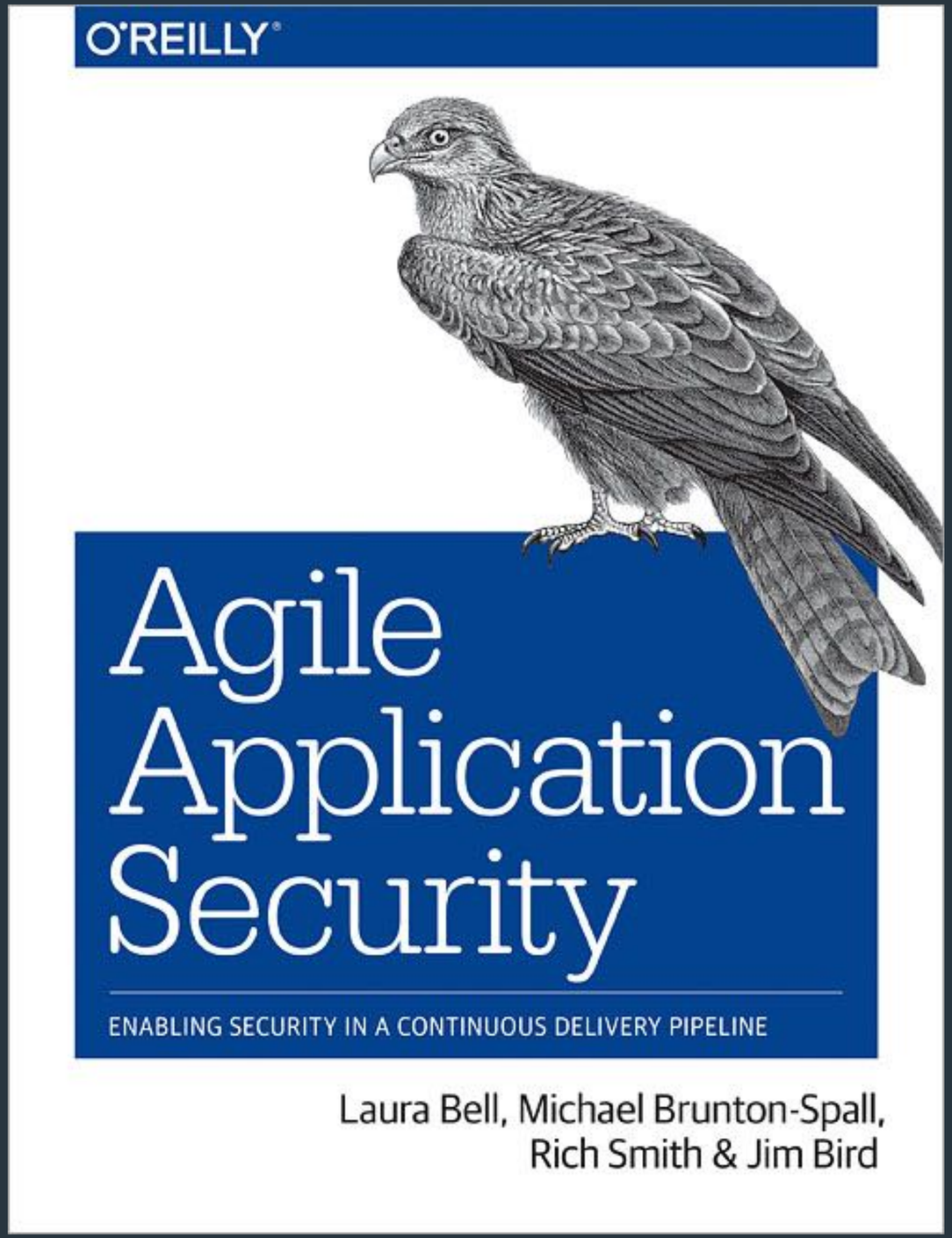
# 2. Reward enthusiasm and aptitude

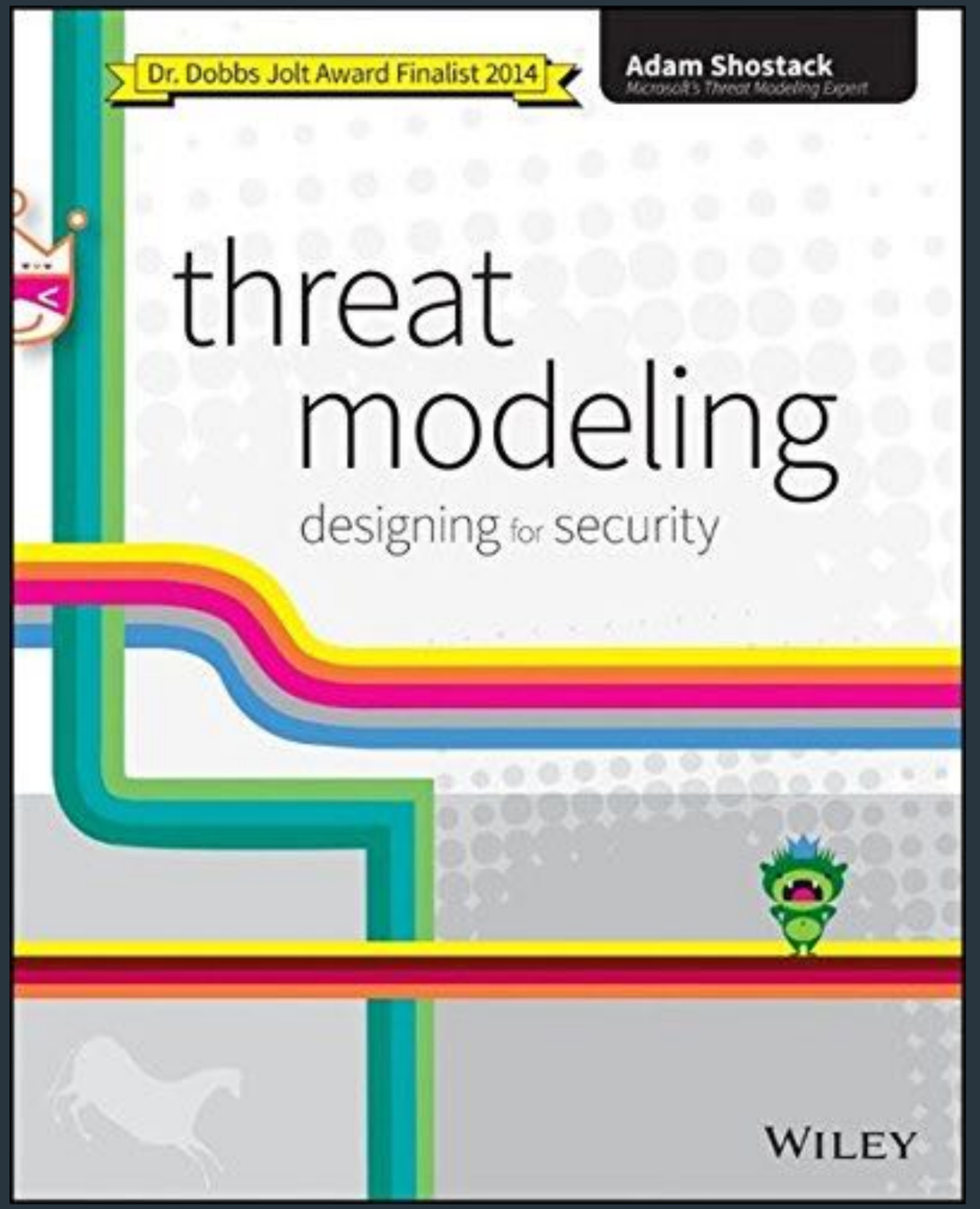
Pair people up across disciplines; provide training; allow experimentation

# 3. Make it very visible

Create an open culture; demonstrate that you welcome critique and are learning

# 4. Invest in spaces and tooling to make this easier


O'REILLY
Agile Application Security
ENABLING SECURITY IN A CONTINUOUS DELIVERY PIPELINE
Laura Bell, Michael Brunton-Spall,
Rich Smith & Jim Bird


Dr. Dobbs Jolt Award Finalist 2014
Adam Shostack
Microsoft's Threat Modeling Expert
threat modeling
designing for security
WILEY

- http://www.cert.org/incident-management/national-csirts/national-csirts.cfm
- https://www.alienvault.com/open-threat-exchange
- https://developers.facebook.com/products/threat-exchange


https://www.safaribooksonline.com/library/view/oreilly-security-conference/9781491976128/video290043.html


https://www.oreilly.com/ideas/operationalizing-security-risk


https://www.ncsc.gov.uk/information/people-strongest-link

https://www.ncsc.gov.uk/blog-post/growing-positive-security-cultures

# Any questions?

James Stewart | @jystewart | james@jystewart.net