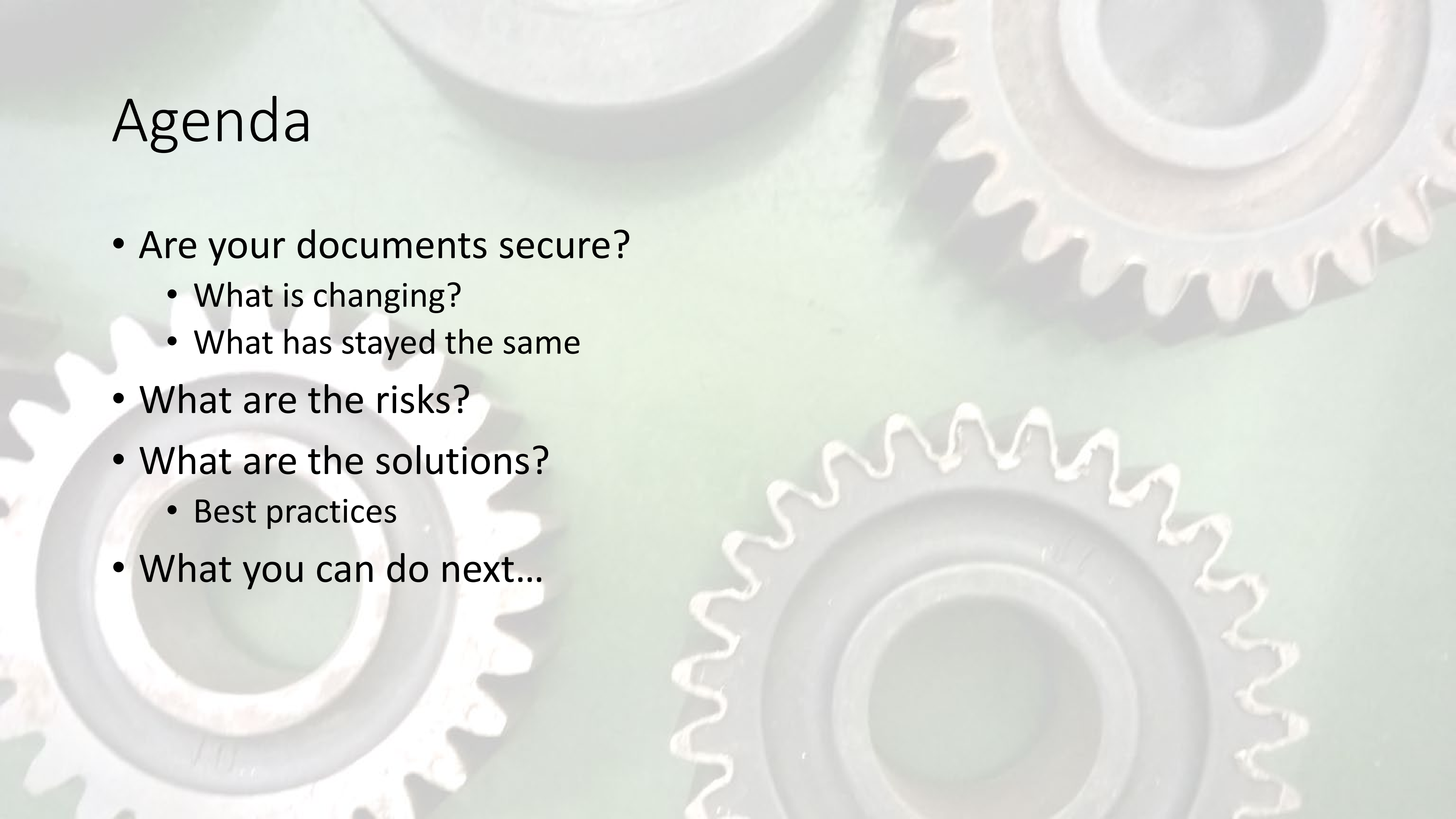
Cybersecurity & documentation: security considerations for authors

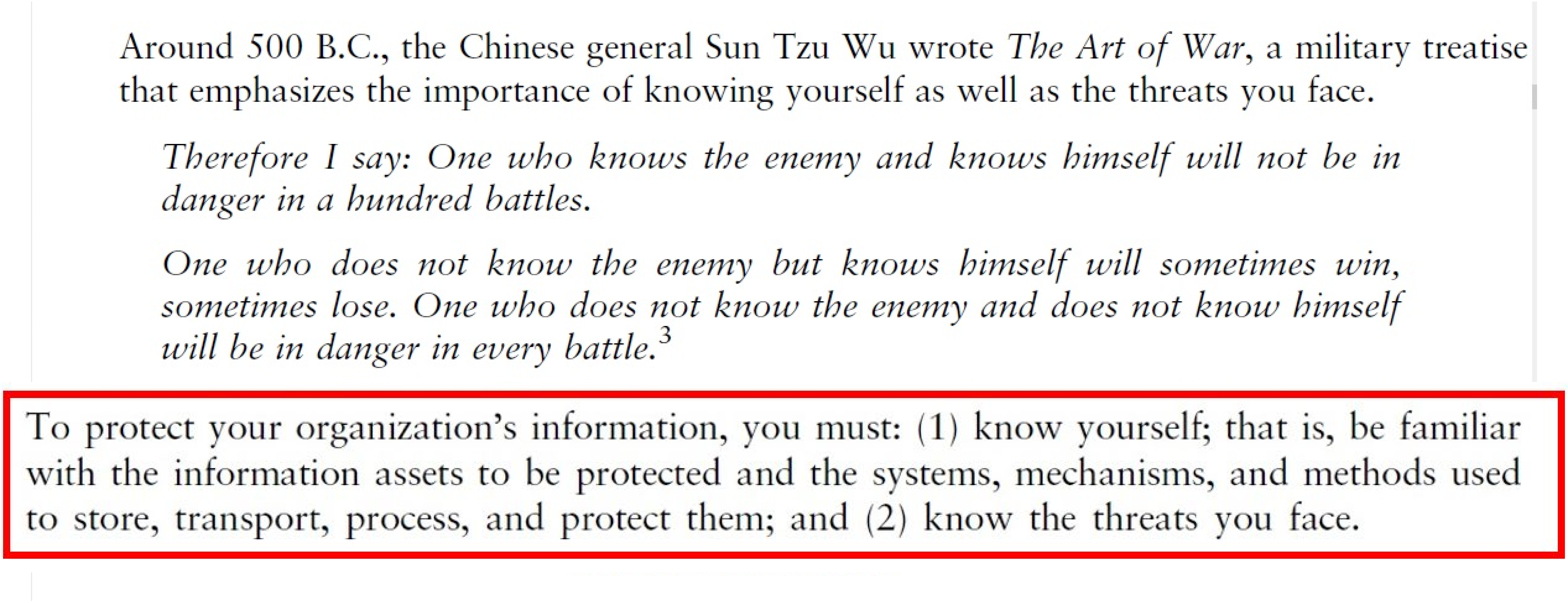
Bridget Khursheed TCUK 2018



Agenda

- Are your documents secure?
  - What is changing?
  - What has stayed the same
- What are the risks?
- What are the solutions?
  - Best practices
- What you can do next…

Security: what is changing?

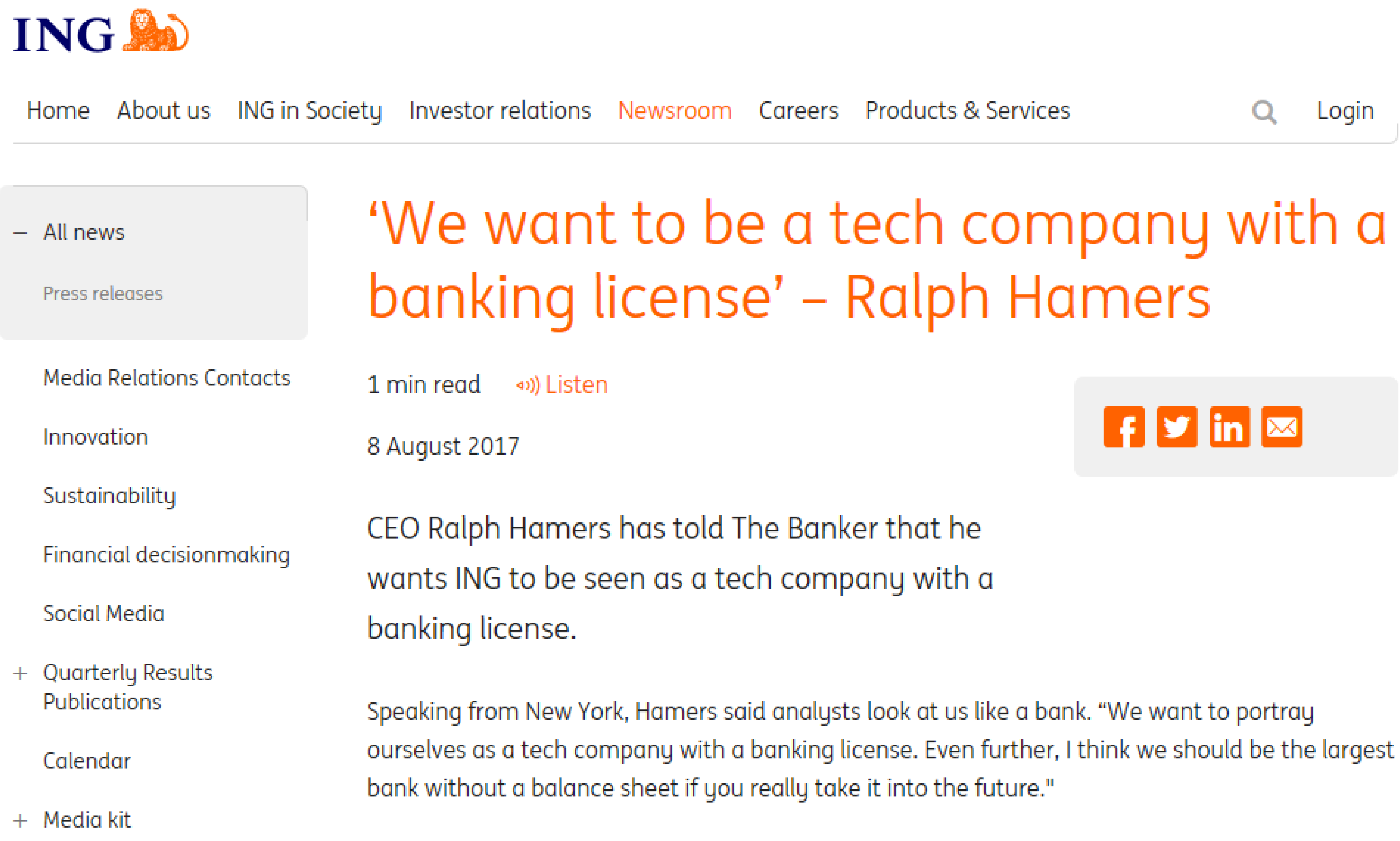


Around 500 B.C., the Chinese general Sun Tzu Wu wrote *The Art of War*, a military treatise that emphasizes the importance of knowing yourself as well as the threats you face.

> *Therefore I say: One who knows the enemy and knows himself will not be in danger in a hundred battles.*
>
> *One who does not know the enemy but knows himself will sometimes win, sometimes lose. One who does not know the enemy and does not know himself will be in danger in every battle.*[3]

To protect your organization's information, you must: (1) know yourself; that is, be familiar with the information assets to be protected and the systems, mechanisms, and methods used to store, transport, process, and protect them; and (2) know the threats you face.

Every company is a software company



‘We want to be a tech company with a banking license’ – Ralph Hamers

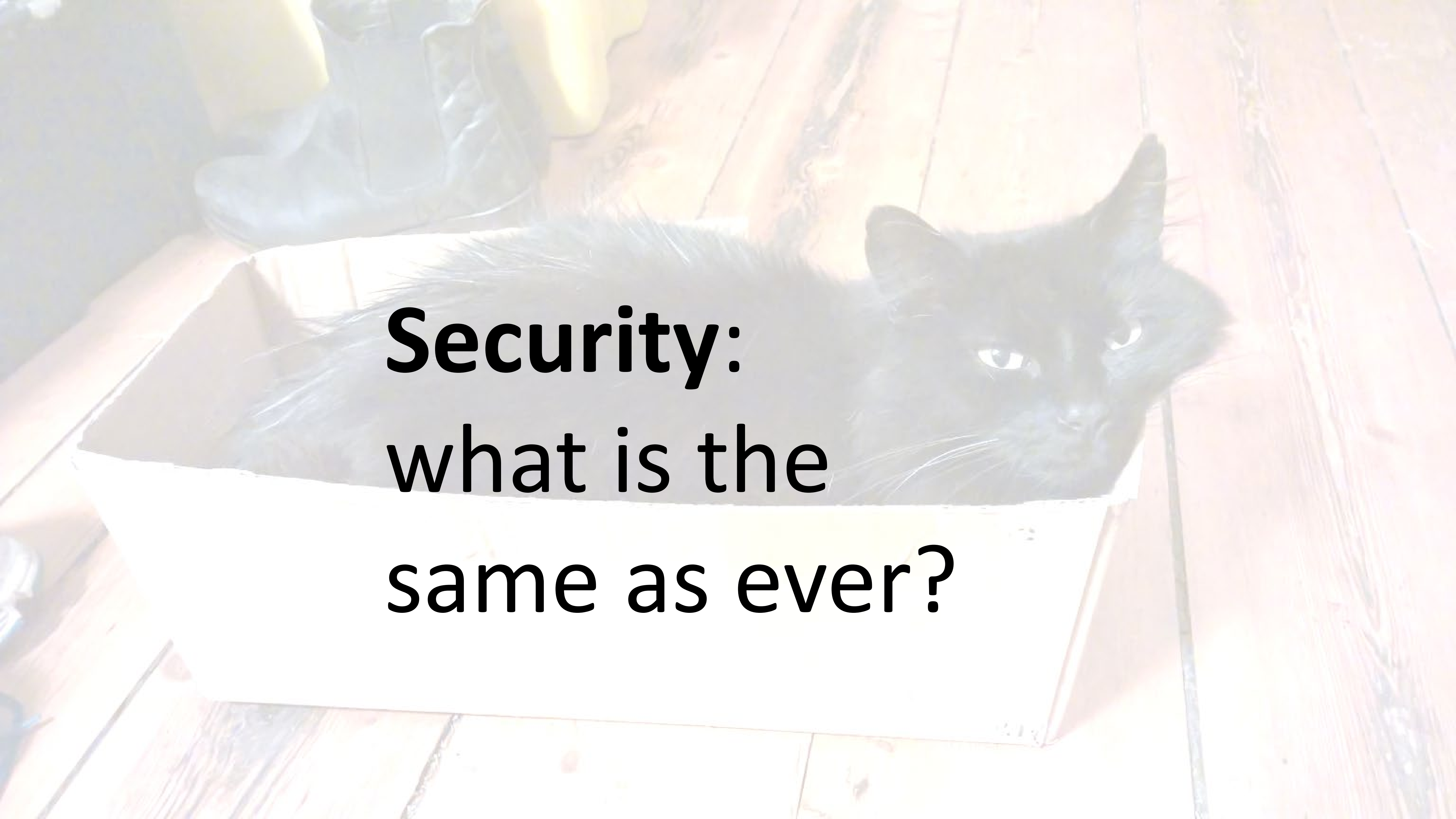
1 min read

8 August 2017

CEO Ralph Hamers has told The Banker that he wants ING to be seen as a tech company with a banking license.

Speaking from New York, Hamers said analysts look at us like a bank. “We want to portray ourselves as a tech company with a banking license. Even further, I think we should be the largest bank without a balance sheet if you really take it into the future."

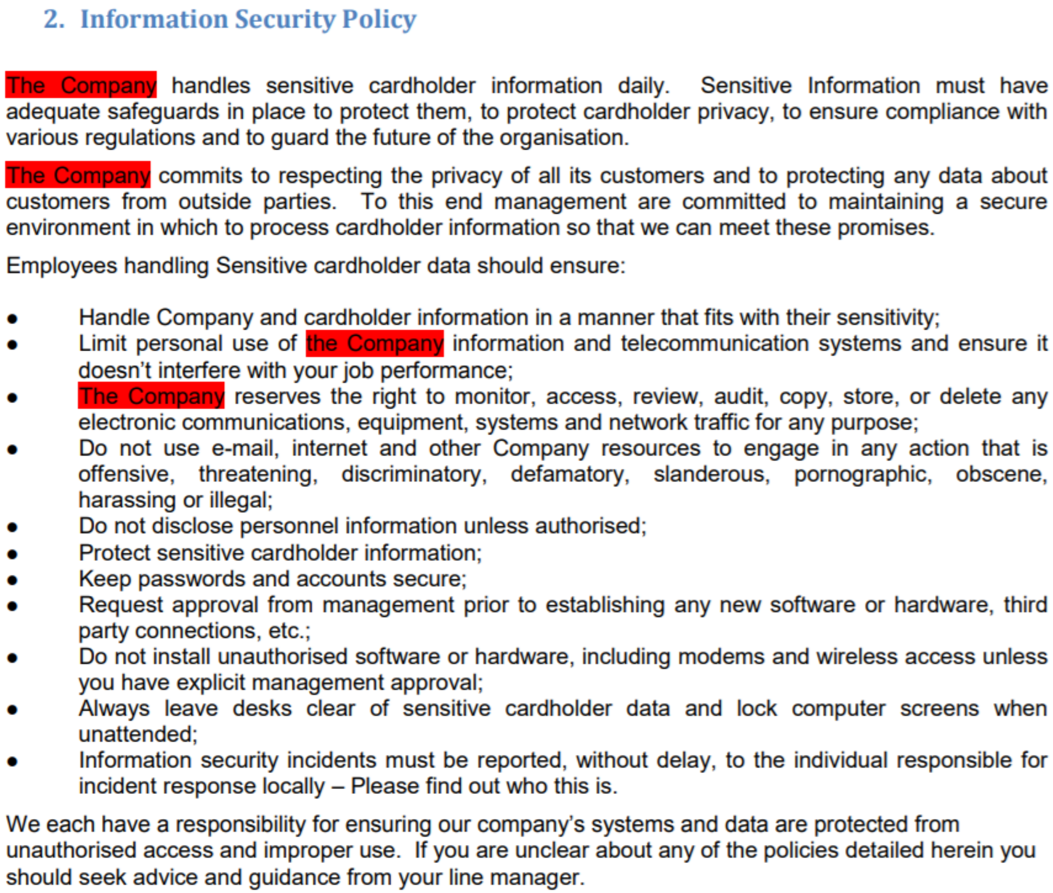
GDPR



Security: what is the same as ever?

Why your docs are already a target

Instagram, Facebook, Cambridge Analytica, profiling etc



2. Information Security Policy

The Company handles sensitive cardholder information daily. Sensitive Information must have adequate safeguards in place to protect them, to protect cardholder privacy, to ensure compliance with various regulations and to guard the future of the organisation.

The Company commits to respecting the privacy of all its customers and to protecting any data about customers from outside parties. To this end management are committed to maintaining a secure environment in which to process cardholder information so that we can meet these promises.

Employees handling Sensitive cardholder data should ensure:

- Handle Company and cardholder information in a manner that fits with their sensitivity;
- Limit personal use of the Company information and telecommunication systems and ensure it doesn't interfere with your job performance;
- The Company reserves the right to monitor, access, review, audit, copy, store, or delete any electronic communications, equipment, systems and network traffic for any purpose;
- Do not use e-mail, internet and other Company resources to engage in any action that is offensive, threatening, discriminatory, defamatory, slanderous, pornographic, obscene, harassing or illegal;
- Do not disclose personnel information unless authorised;
- Protect sensitive cardholder information;
- Keep passwords and accounts secure;
- Request approval from management prior to establishing any new software or hardware, third party connections, etc.;
- Do not install unauthorised software or hardware, including modems and wireless access unless you have explicit management approval;
- Always leave desks clear of sensitive cardholder data and lock computer screens when unattended;
- Information security incidents must be reported, without delay, to the individual responsible for incident response locally – Please find out who this is.

We each have a responsibility for ensuring our company's systems and data are protected from unauthorised access and improper use. If you are unclear about any of the policies detailed herein you should seek advice and guidance from your line manager.

Source: WorldPay WPUK-SaferPayments-Information-Security-Policy template

But what if the definition of information that needs to be kept safe is a little fuzzier? How does this affect authors?

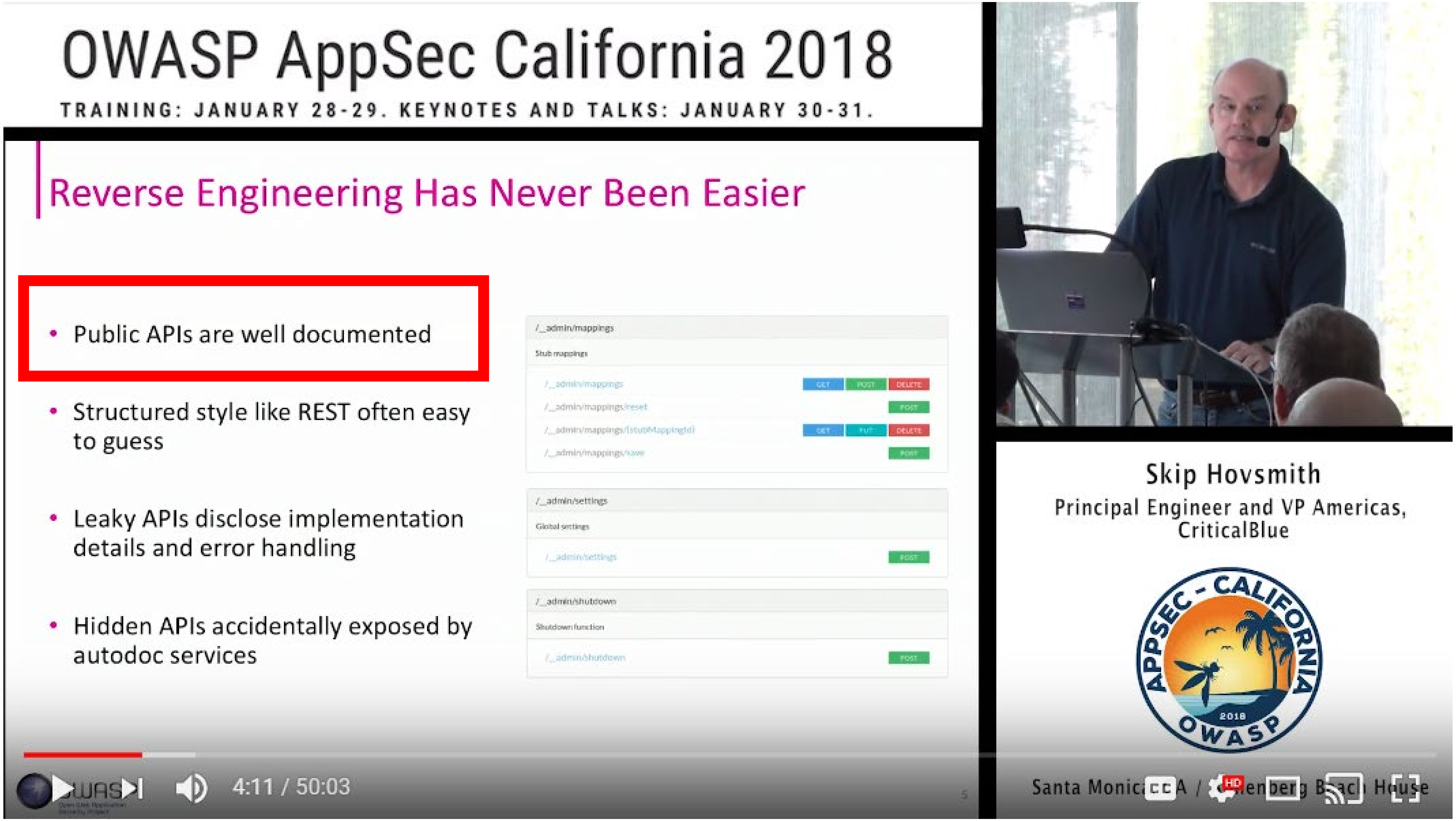
Why your API is already a target

- Global API attack landscape is lucrative, mature and well-defined
- **“APIs are the first place we look”**
  Stuart Peck OPSEC expert ZERODAYLABS

e.g. Microsoft currently has 3500 security professionals handling 6.5 trillion events a day (24 SEP 2018)

What do attackers get out of it?

Open-source intelligence (**OSINT**) is data collected from publicly available sources to be used in an intelligence context. In the intelligence community, the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources).



OWASP AppSec California 2018

TRAINING: JANUARY 28-29. KEYNOTES AND TALKS: JANUARY 30-31.

Reverse Engineering Has Never Been Easier

- Public APIs are well documented
- Structured style like REST often easy to guess
- Leaky APIs disclose implementation details and error handling
- Hidden APIs accidentally exposed by autodoc services

/__admin/mappings

Stub mappings

/__admin/mappings	GET POST DELETE
/__admin/mappings/reset	POST
/__admin/mappings/{stubMappingId}	GET PUT DELETE
/__admin/mappings/save	POST

/__admin/settings

Global settings

/__admin/settings	POST

/__admin/shutdown

Shutdown function

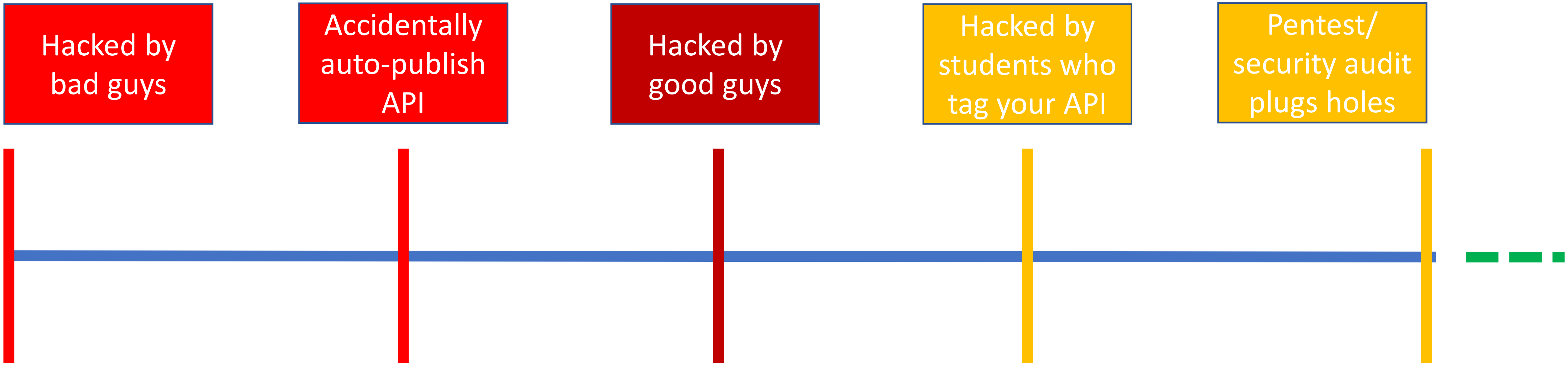
/__admin/shutdown	POST

Skip Hovsmith

Principal Engineer and VP Americas, CriticalBlue

Security:
what are the risks?

Spectrum of vulnerability



Hacked by bad guys

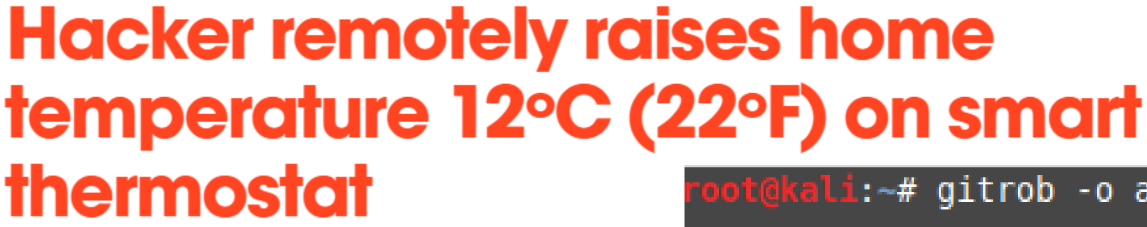
Accidentally auto-publish API

Hacked by good guys

Hacked by students who tag your API

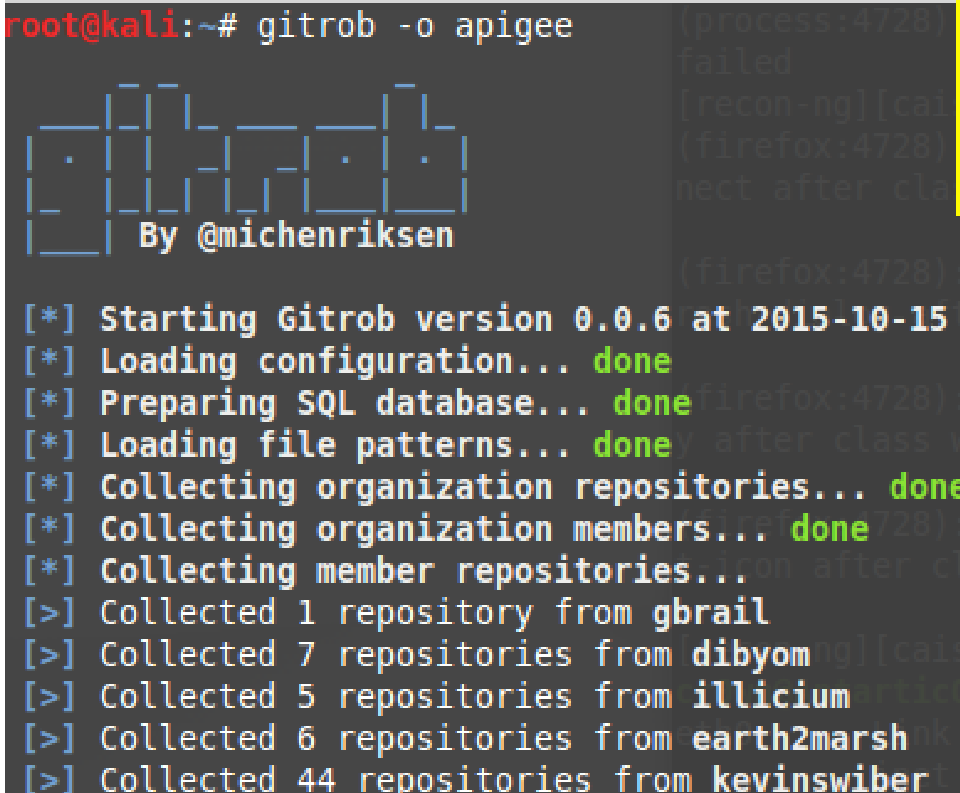
Pentest/ security audit plugs holes

Attacks

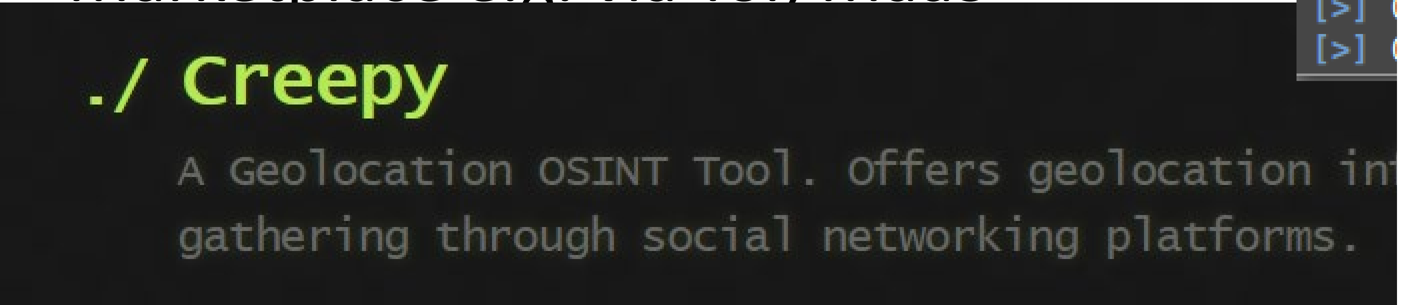


Hacker remotely raises home temperature 12°C (22°F) on smart thermostat

- Social engineering
  - Phishing, geolocation, data gathering, observation
  - Software tools e.g. LinkedIn, Creepy, Iknowwhereyourcatlives.com, Snap Maps
- Software to scrape information
  - e.g. GitRob, Strava data analysis
- Software to control information
  - e.g IoT malware
- Marketplace e.g. via Tor, MaaS

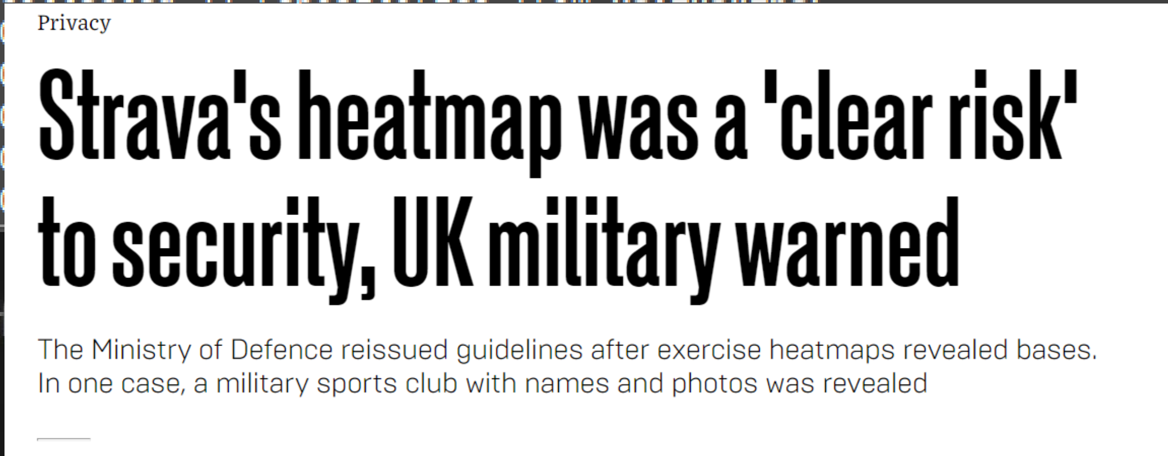


```
root@kali:~# gitrob -o apigee
         _ _           _
     ___|_| |_ ___ ___| |_
    | . | |  _|  _| . | . |
    |_  |_|_| |_| |___|___|
    |___| By @michenriksen

[*] Starting Gitrob version 0.0.6 at 2015-10-15 07:19 PDT
[*] Loading configuration... done
[*] Preparing SQL database... done
[*] Loading file patterns... done
[*] Collecting organization repositories... done
[*] Collecting organization members... done
[*] Collecting member repositories...
[>] Collected 1 repository from gbrail
[>] Collected 7 repositories from dibyom
[>] Collected 5 repositories from illicium
[>] Collected 6 repositories from earth2marsh
[>] Collected 44 repositories from kevinswiber
[>]
[>]
[>]
[>]
[>]
```



./ Creepy

A Geolocation OSINT Tool. Offers geolocation in
gathering through social networking platforms.

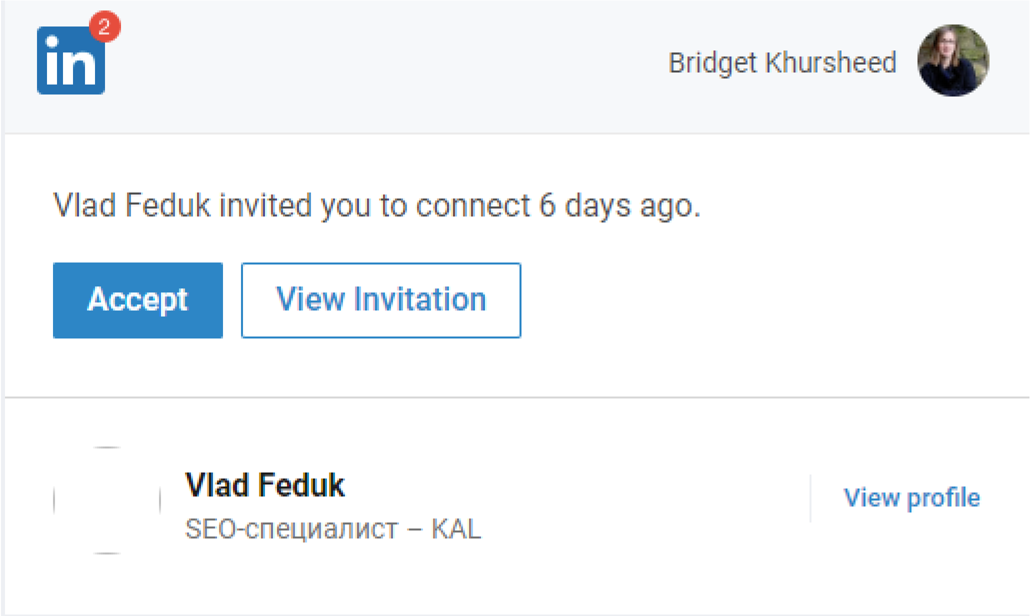


Privacy

Strava's heatmap was a 'clear risk' to security, UK military warned

The Ministry of Defence reissued guidelines after exercise heatmaps revealed bases. In one case, a military sports club with names and photos was revealed

Spearphishing

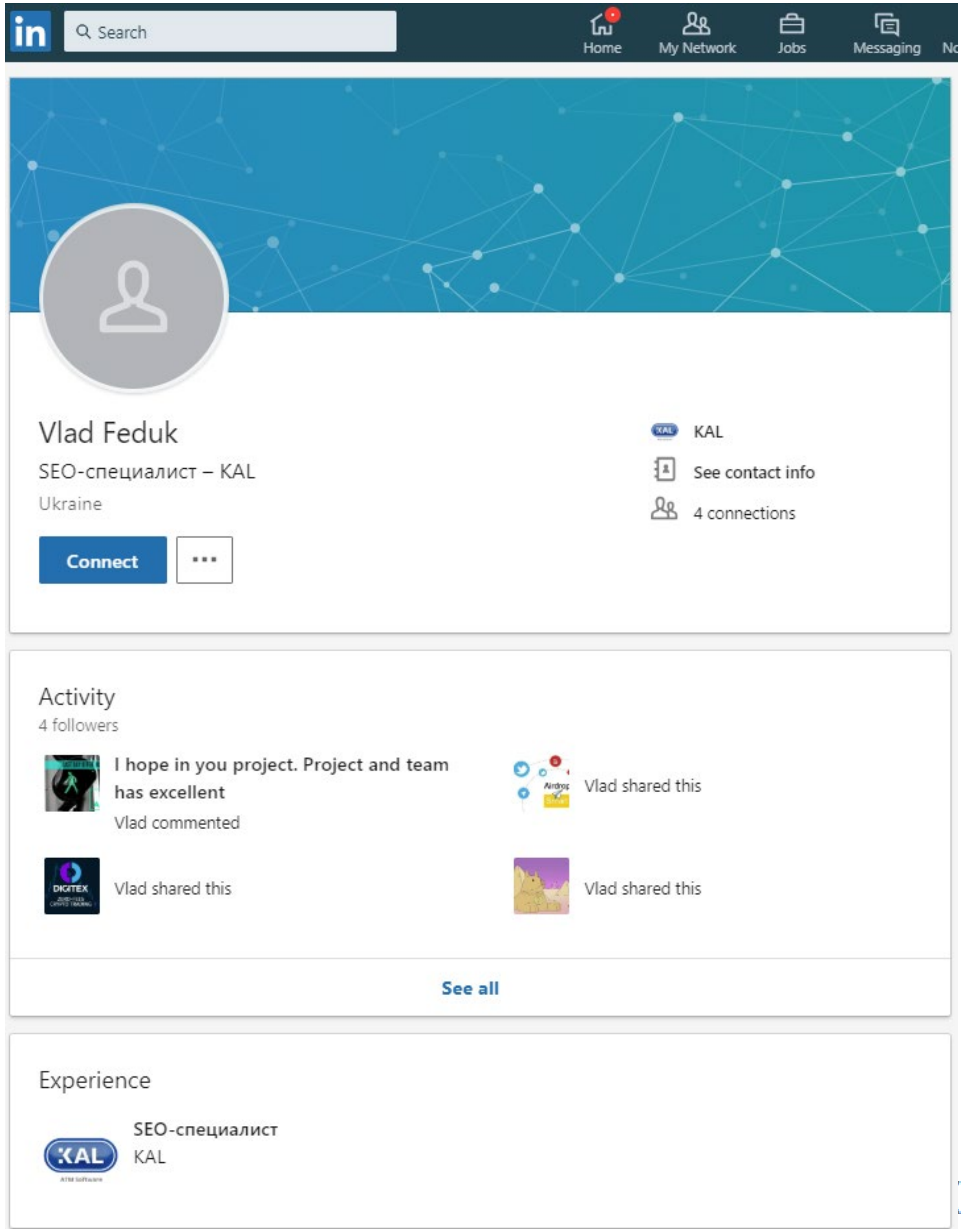


Bridget Khursheed

Vlad Feduk invited you to connect 6 days ago.

Vlad Feduk

SEO-специалист – KAL



Vlad Feduk

SEO-специалист – KAL

Ukraine

KAL

See contact info

4 connections

Activity

4 followers

I hope in you project. Project and team has excellent

Vlad commented

Vlad shared this

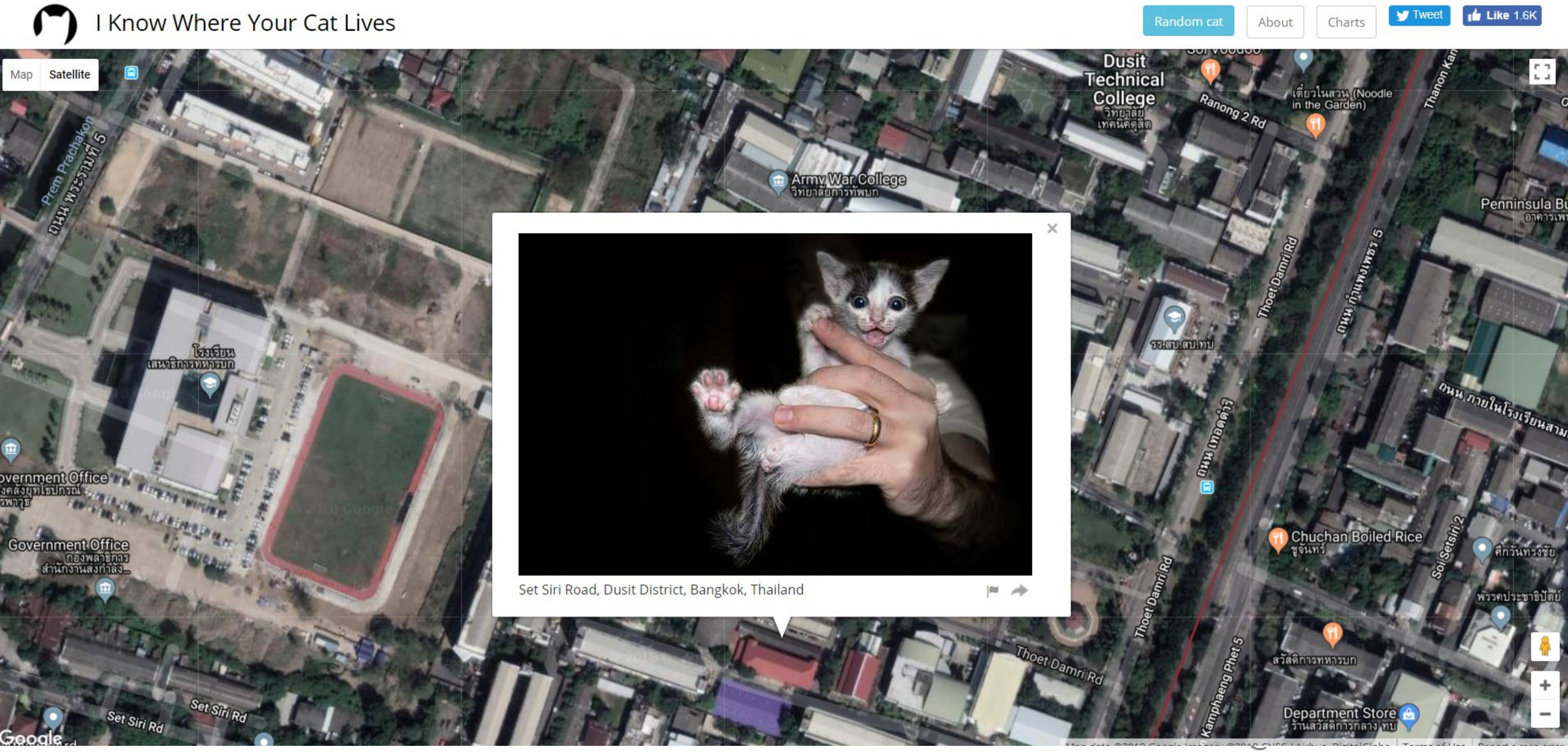
Vlad shared this

Vlad shared this

Experience

SEO-специалист

KAL

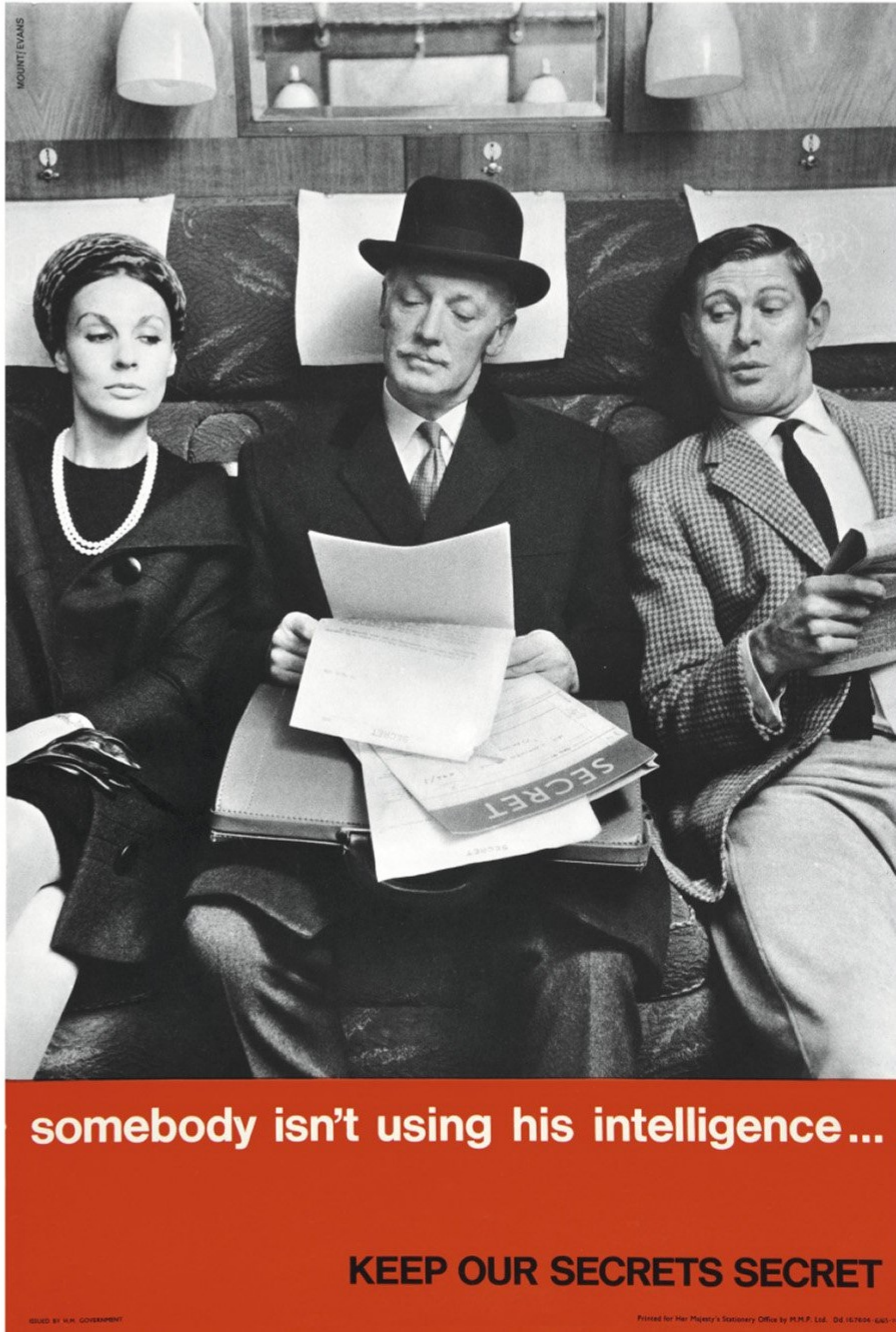


I Know Where Your Cat Lives

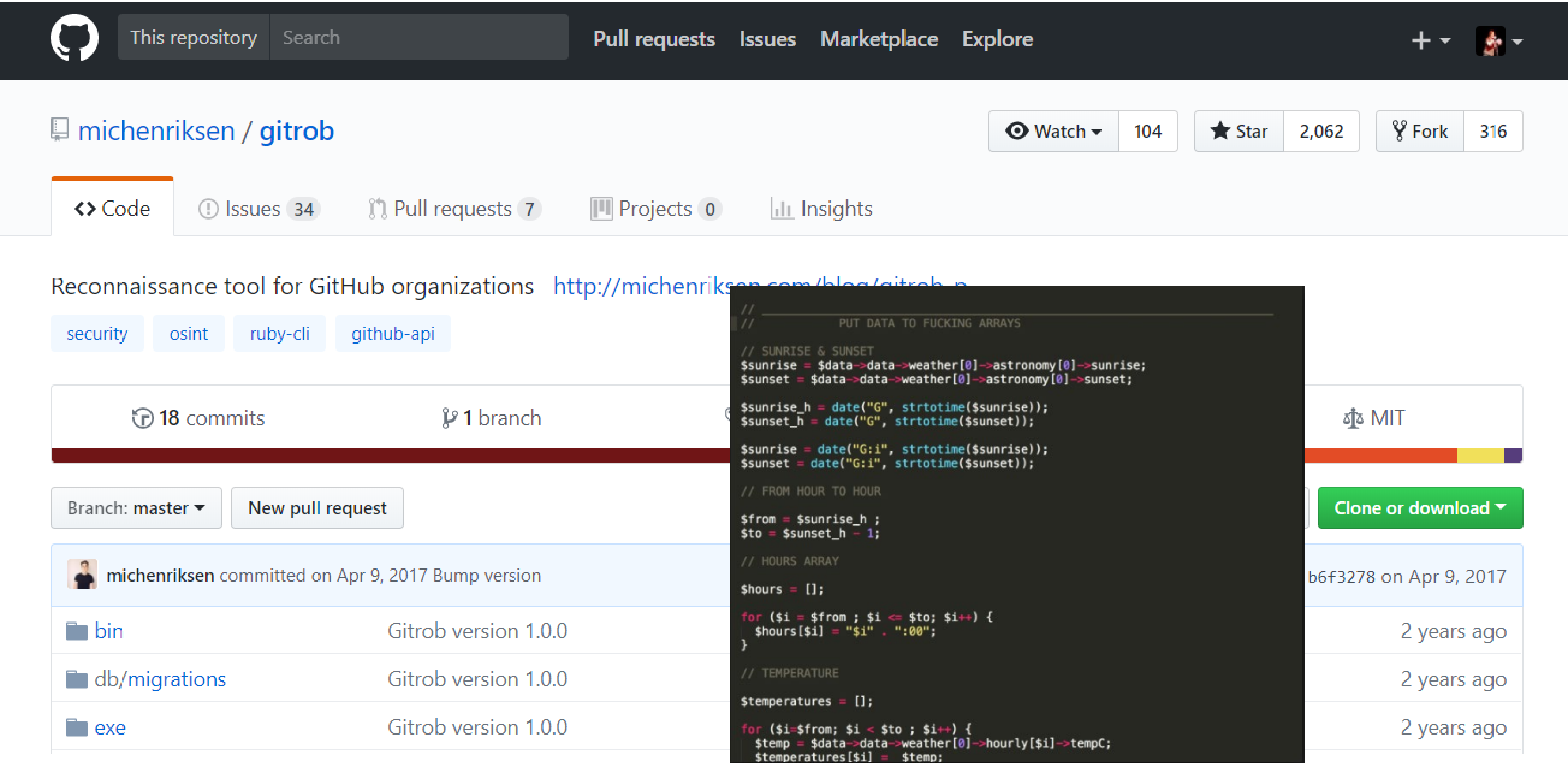
Set Siri Road, Dusit District, Bangkok, Thailand

APIs that give the game away

- Cultural giveaways
- Non-professional
- Auto-generation tools
  - What could go wrong?!
- Vulnerabilities include:
  - Certificates: e.g. training users to click popups or accept the fact that the certificate isn't right
  - Loosely defined or leaky data
    - Type checking, assertions, root level access
  - Endpoints especially legacy endpoints, multiple APIs
- Liability?


MOUNT/EVANS
SECRET
somebody isn't using his intelligence...
KEEP OUR SECRETS SECRET
ISSUED BY H.M. GOVERNMENT
Printed for Her Majesty's Stationery Office by M.M.P. Ltd.

Being professional



michenriksen / gitrob

Reconnaissance tool for GitHub organizations http://michenriksen.com/blog/gitrob-p

security osint ruby-cli github-api

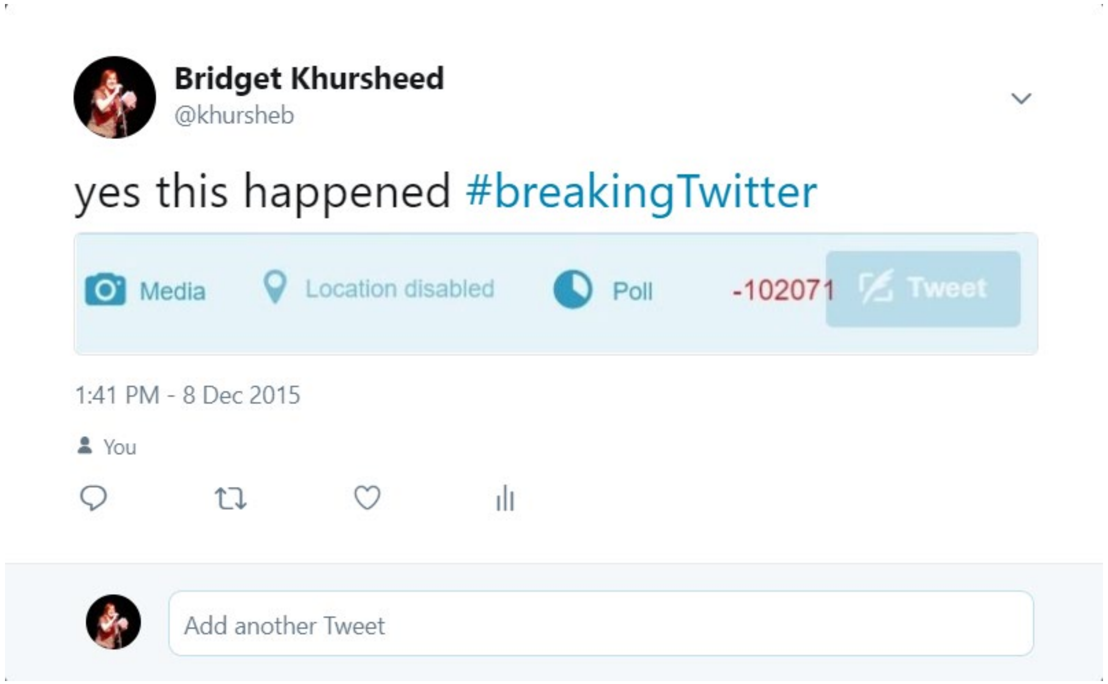
18 commits 1 branch MIT

michenriksen committed on Apr 9, 2017 Bump version b6f3278 on Apr 9, 2017

bin	Gitrob version 1.0.0	2 years ago
db/migrations	Gitrob version 1.0.0	2 years ago
exe	Gitrob version 1.0.0	2 years ago

```
// ____________________________________________________________
//              PUT DATA TO FUCKING ARRAYS

// SUNRISE & SUNSET
$sunrise = $data->data->weather[0]->astronomy[0]->sunrise;
$sunset = $data->data->weather[0]->astronomy[0]->sunset;

$sunrise_h = date("G", strtotime($sunrise));
$sunset_h = date("G", strtotime($sunset));

$sunrise = date("G:i", strtotime($sunrise));
$sunset = date("G:i", strtotime($sunset));

// FROM HOUR TO HOUR

$from = $sunrise_h ;
$to = $sunset_h - 1;

// HOURS ARRAY

$hours = [];

for ($i = $from ; $i <= $to; $i++) {
  $hours[$i] = "$i" . ":00";
}

// TEMPERATURE

$temperatures = [];

for ($i=$from; $i < $to ; $i++) {
  $temp = $data->data->weather[0]->hourly[$i]->tempC;
  $temperatures[$i] =  $temp;
```

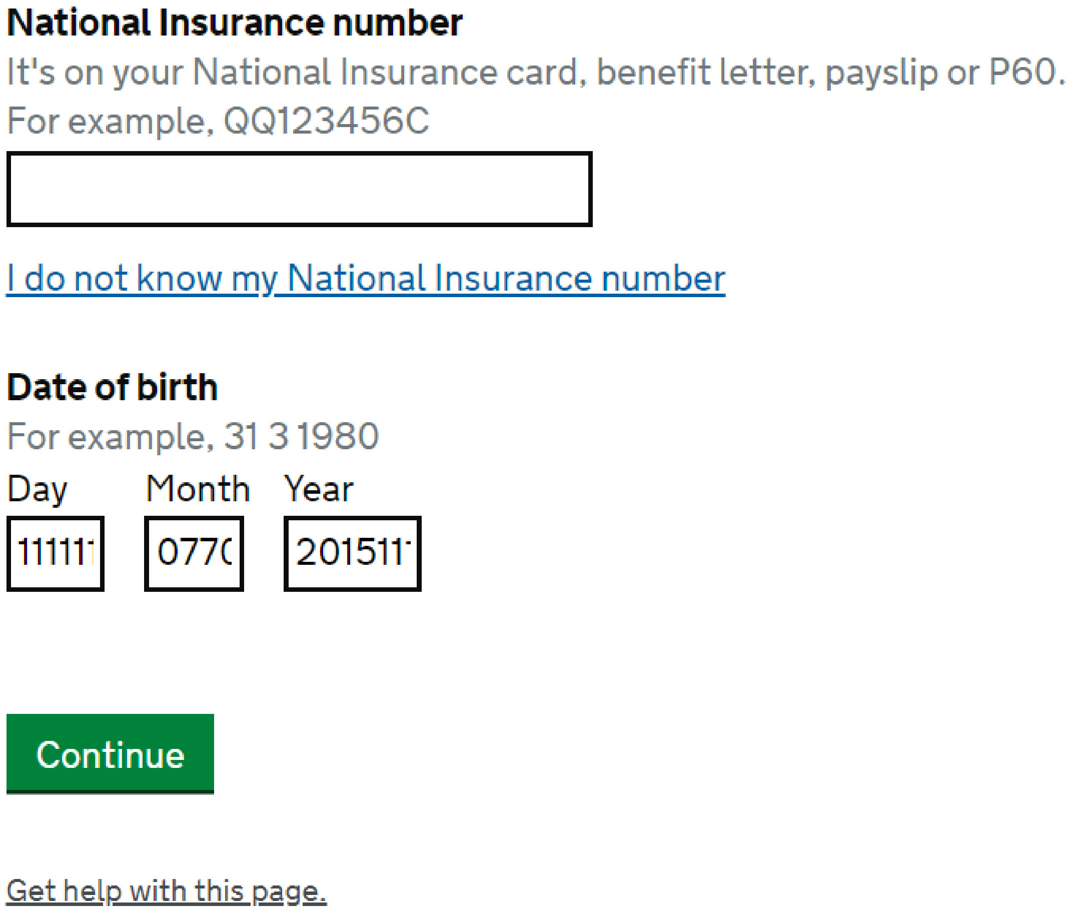
Example data input parameters not checked



Bridget Khursheed
@khursheb

yes this happened #breakingTwitter

1:41 PM - 8 Dec 2015



National Insurance number

It's on your National Insurance card, benefit letter, payslip or P60.
For example, QQ123456C

I do not know my National Insurance number

Date of birth

For example, 31 3 1980

Day	Month	Year
11111	077	201511

Get help with this page.

Worked example Facebook courtesy of **Laxman Muthiyah** zerohacks

Initial attempt:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=CAACEd…..MUZD

Response :-
{“error”:{“message”:”(#200) Application does not have the capability to make this API call.”,”type”:”OAuthException”,”code”:200}}
```

Next attempt:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=<Facebook_for_Android_Access_Token>

Response:-
true
```

Final attempt on victim:

```
Request :-
DELETE /518171421550249 HTTP/1.1
Host :  graph.facebook.com
Content-Length: 245
access_token=<Facebook_for_Android_Access_Token>

Response:-
true
```

https://zerohacks.com/bug-bounty-hacks/how-i-hacked-your-facebook-photos/
last modified 19.03.18

Security: what are the solutions?

Is security a consideration for your API?

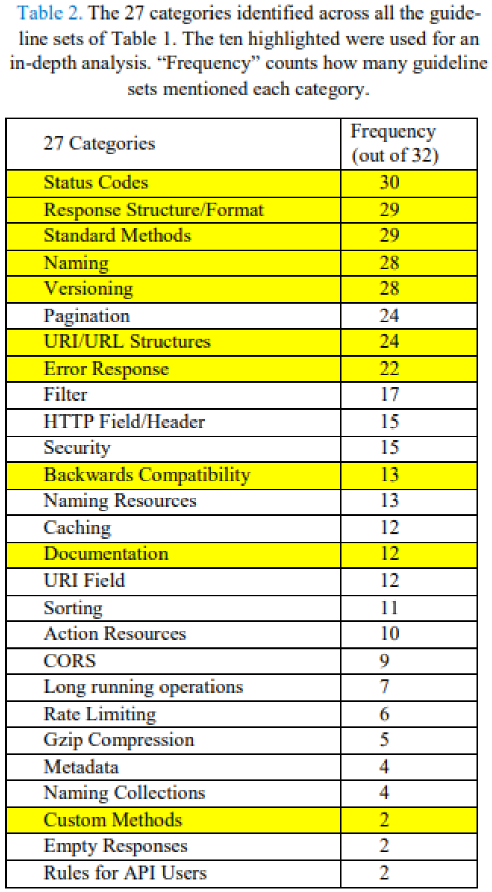


Table 2. The 27 categories identified across all the guideline sets of Table 1. The ten highlighted were used for an in-depth analysis. “Frequency” counts how many guideline sets mentioned each category.

27 Categories	Frequency (out of 32)
Status Codes	30
Response Structure/Format	29
Standard Methods	29
Naming	28
Versioning	28
Pagination	24
URI/URL Structures	24
Error Response	22
Filter	17
HTTP Field/Header	15
Security	15
Backwards Compatibility	13
Naming Resources	13
Caching	12
Documentation	12
URI Field	12
Sorting	11
Action Resources	10
CORS	9
Long running operations	7
Rate Limiting	6
Gzip Compression	5
Metadata	4
Naming Collections	4
Custom Methods	2
Empty Responses	2
Rules for API Users	2

- Murphy, L., Alliyu, T., Macvean, A., Kery, M. B., & Myers, B. A. (2017). Preliminary Analysis of REST API Style Guidelines. *PLATEAU’17 Workshop on Evaluation and Usability of Programming Languages and Tools*. Retrieved from http://www.cs.cmu.edu/~NatProg/papers/API-Usability-Styleguides-PLATEAU2017.pdf

courtesy of Pronovix newsletter ☺

Best practices

Training in API security & social engineering

For developers/security policy include:

- Writing restrictions e.g. Least privilege policy
- Secure authentication
- Regular security audit/PEN test – this should include documentation review

For API documentarians include:

- OPSEC obfuscation
  - Abstraction e.g. no examples from own company culture, multiple code examples, don’t specify the sourcecode language
  - Hide data specifics where possible e.g. No passwords obvs but also pseudocode, obscure GETs examples, email format etc
- Backup files – check for inappropriate content
- Watch out for features that train users to be less secure
- Handle auto-gen with care

All authors

- **Learn (some) code ☺**
- **Become cybersecurity aware** e.g. Attend your local security meetup, chat on Slack, Discord etc.

Moving targets

- PSD2 opens banking interfaces offers lucrative opportunities for organised crime (January 2018)

The survey respondents indicated that the risk of fraud arising from third-party access to accounts is a serious concern and that fraud prevention is a top priority. McKinsey

Payment Initiation Service Providers (PISP) – 3rd party providers can initiate payment on behalf of a consumer. **Account Information Service Providers (AISP)** – 3rd party providers can now access bank account information. ***"One nice feature is all your financial information appears in one place."***

What you can do next

Doc Managers

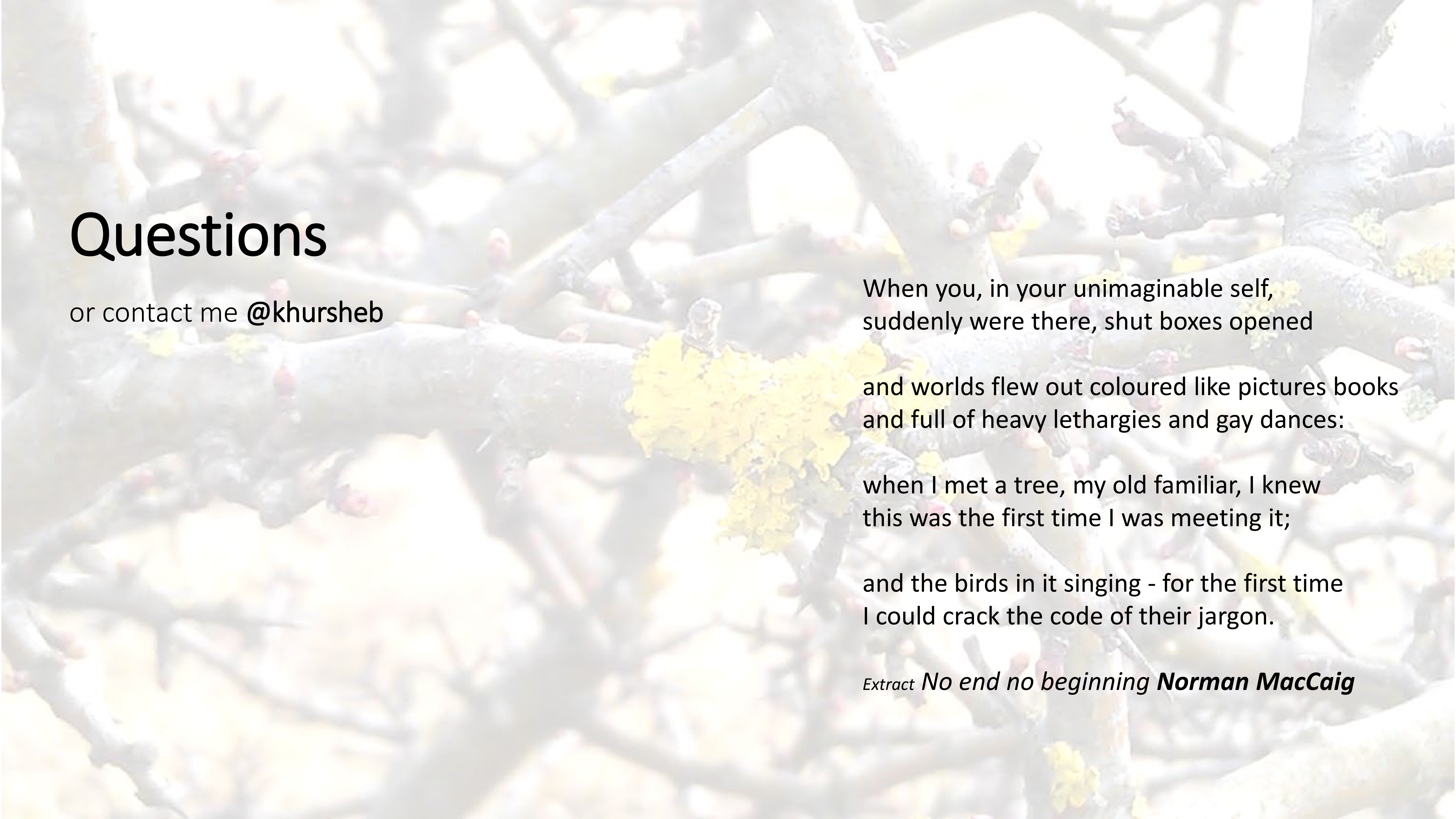
- Locate Corporate Information Security Policy (CISP)
- Join the security conversation e.g. “security as a user experience issue”
- Develop explicit doc security strategy

Authors

- Be scrupulous – you may be a target
- Avoid giving too much away
- Software error analysis

Freelancers

- Create your own CISP
- Security audit of systems
- Monitor risk e.g. email



Questions

or contact me **@khursheb**

When you, in your unimaginable self,
suddenly were there, shut boxes opened

and worlds flew out coloured like pictures books
and full of heavy lethargies and gay dances:

when I met a tree, my old familiar, I knew
this was the first time I was meeting it;

and the birds in it singing - for the first time
I could crack the code of their jargon.

Extract No end no beginning ***Norman MacCaig***

References

- OPSEC talk Stuart Peck (ZeroDayLab) Edinburgh Security Meetup 29th March 2018
- PSD2: Taking advantage of open-banking disruption By Alessio Botta, Nunzio Digiacomo, Reinhard Höll, and Liz Oakes (McKinsey) January 2018 accessed March 2018 https://www.mckinsey.com/industries/financial-services/our-insights/psd2-taking-advantage-of-open-banking-disruption
- Information security policy template: WorldPay WPUK-SaferPayments-Information-Security-Policy http://www.worldpay.com/sites/default/files/WPUK-SaferPayments-Information-Security-Policy.pdf
- Hacker thermostat Nextweb July 21 2017 https://thenextweb.com/insider/2017/07/21/hacker-remotely-raises-home-temperature-12oc-22of-smart-thermostat/
- Gifs: 21 Jump Street Original Film/SJC Studios; Napoleon Dynamite MTV Films/Dynamite Films/Access Films
- Skip Horsvath Critical Blue at Open Web Application Security Project (OWASP) AppSec January 2018 https://www.youtube.com/watch?v=lgAEJwgxe0Y
- Deleting any photo albums – How I Hacked Your Facebook Photos Laxman Muthiyah on ZeroHacks - last modified : March 19 2018 https://zerohacks.com/bug-bounty-hacks/how-i-hacked-your-facebook-photos/
- Microsoft security incident stat PCWorld September 24 2018 https://uk.pcmag.com/news/117564/microsoft-ceo-pushes-open-data-initiative-new-security-at-ig
- Strava's heat map Wired April 4 2018 https://www.wired.co.uk/article/strava-heat-maps-military-app-uk-warning-security
- I know where your cat lives https://iknowwhereyourcatlives.com/cat/d6dbd9dd6a
- Snap Maps risks The Guardian June 23 2017 https://www.theguardian.com/technology/2017/jun/23/snapchat-maps-privacy-safety-concerns