



Shh... Keeping Secrets safe in an Automated Build and Deployment Pipeline

Kristian Bank Erbou
Coding CEO

BuildingBetterSoftware.com
kbe@buildingbettersoftware.com

Agenda

What defines a “secret” in software development

Why secrets are important

How to remain compliant



Kristian Bank Erbou

Coding CEO

15+ years experience developing software

#6 employee in Just-Eat.com

Ebay (Denmark), DGI (Danish NGO), LEGO

Co-Founder of BuildingBetterSoftware.com – we create amazing software and IT organizations

"General Data Protection Regulation"



By gotphotos/shutterstock.com

British Airways databreach (2019)



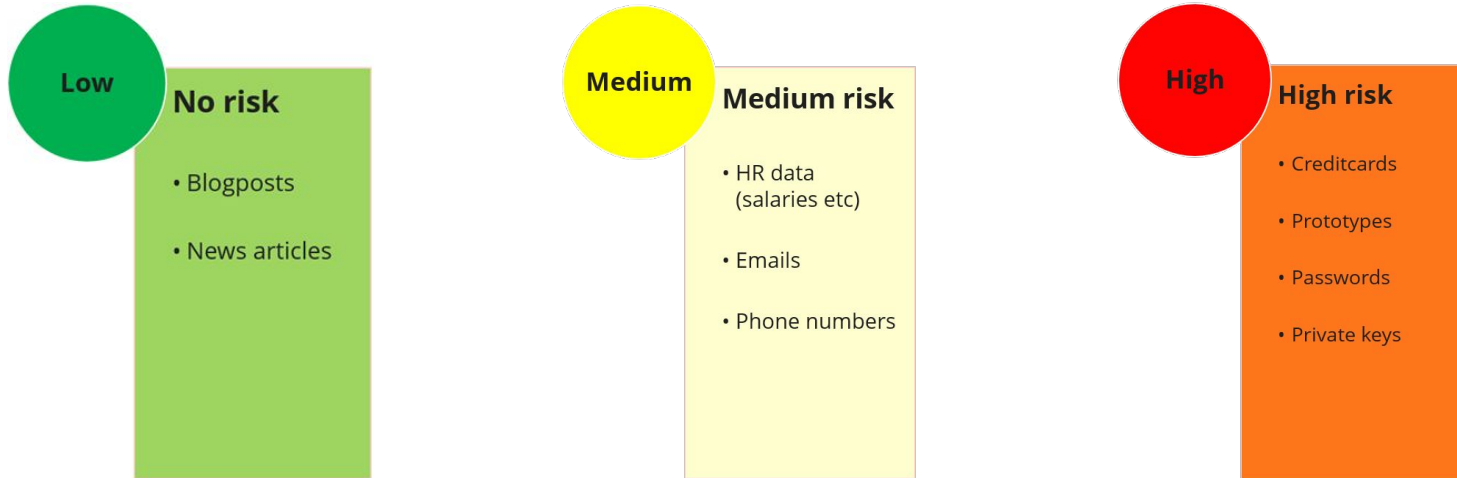
£183.39M fine

“The ICO’s investigation has found that a variety of information was compromised by **poor security arrangements** at the company, including log in, payment card, and travel booking details as well name and address information”

Source: <https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/07/ico-announces-intention-to-fine-british-airways/>

GDPR classification: Risk profile

How much harm will a data breach do to a business and to individuals?




Rule #1: Keep secrets away from sourcecontrol !

Low No risk



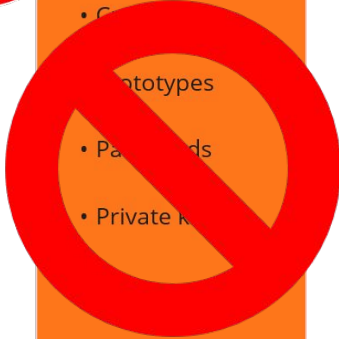
• Credentials

Medium Medium risk



• Phone numbers

High High risk



- Credentials
- Prototypes
- Passwords
- Private keys

Remove secrets from sourcecode

Example of a "config.ini" file in version control:

```
...  
db_timeout_seconds: 60  
db_username: sa_website_foobar  
db_password: PQT9eHq8rhZA  
db_failover_enabled: false  
...
```



```
...  
db_timeout_seconds: 60  
db_username: sa_website_foobar  
db_password: ###DB_PASSWORD###  
db_failover_enabled: false  
...
```

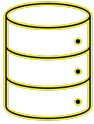


How to keep secrets secret, solution #1

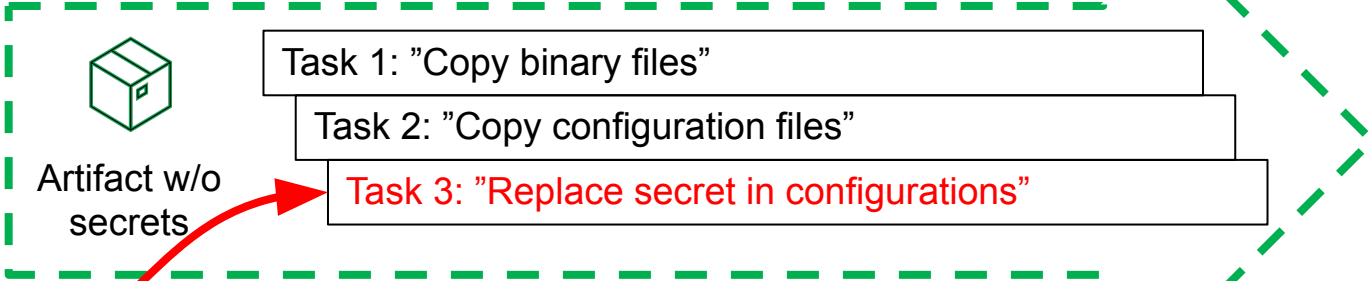


IT Ops

Add encrypted variable to pipeline definition



CI/CD



Delivery team

How to keep secrets secret, solution #2



IT Ops



Secrets

API

Deployment pipeline

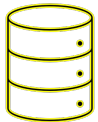


Artifact w/o
secrets

Task 1: "Copy binary files"

Task 2: "Copy configuration files"

Task 3: "Replace secret in configurations"



CI/CD



Delivery team

Privacy by design is a solved problem



Azure Key Vault



AWS Secrets
Manager



Key
Management
Service



HashiCorp
Vault

<https://www.vaultproject.io/use-cases/secrets-management>

<https://azure.microsoft.com/en-us/services/key-vault/>

<https://aws.amazon.com/secrets-manager/>

<https://cloud.google.com/kms>

Summary

Don't go easy on GDPR and privacy

Treat your employer secrets with care

Separating sensitive data from restricted data is a solved problem

Simple is safer – don't roll your own!

Upcoming book 2020-Q3 w/foreword by Jayne Groll

THANK YOU!

Meet me in the Network
Chat Lounge for questions