

Starting shortly.  
Please wait!

# Top 5 data security risks

For M&E Specialists



ActivityInfo

# Introductions - ActivityInfo

**ActivityInfo** Search for a database, folder or form...

DATABASES > YECRP > SUBPROJECTS

**Subprojects** Form settings

+ Add record Import Export Select columns Map

Project code	Implementing ...	Governorate Na...	District Name	LATITUDE Geographic location
PR0507	PWP	Taiz	Mawza	13.256760
<b>PR0677</b>	<b>PWP</b>	<b>Sanaa</b>	<b>Nihm</b>	<b>15.556346</b>
PR0909	SFD	Ibb	Al Mashannah	13.977640
PR0671	PWP	Ad Dali	Damt	14.206364
PR0744	PWP	Dhamar	Otmah	14.497551
PR0416	SFD	Sanaa	Al Haymah Ad Da...	15.279392
PR0533	PWP	Taiz	Mawiyah	13.580590
PR0723	PWP	Dhamar	Dwran Anis	14.676763
PR0173	PWP	Hajjah	Ash Shahil	15.880991
PR0200	SFD	Al Bayda	Al Bayda City	13.979086

**Record** Collapse >

Print record Edit record Delete record

**Details**

Go to subform: Monthly p Disburse

PROJECT CODE PR0677 IMPLEMENTING PART PWP


**ActivityInfo** Search for a database, folder or form...

DATABASES > YECRP > SUBPROJECTS

**Subprojects** Form settings

+ Add record Import Return to table

Geography: Geographic location Satellite basemap



**Record** Collapse >

PROJECT CODE PR0098

IMPLEMENTING PARTNER PWP

LOCATION Al Chaydhah Al Maharah

GEOGRAPHIC LOCATION 16° 13' 36.70" N, 52° 11' 15.29" E

SUB-PROJECT TYPE Road rehabilitation

BUDGET 30000 USD

NUMBER OF DIRECT BENEFICIARIES 2205

NUMBER OF INDIRECT BENEFICIARIES 8820

PERCENTAGE OF DIRECT BENEFICIARIES THAT ARE WOMEN 90



# What is data security?

- » **Confidentiality**

Confidential data exposed to unauthorized parties

- » **Integrity**

Data changed without your permission

- » **Availability**

Ensuring data is available when needed



# Top Five Risks

#5 Social engineering

#4 Password management

#3 IT operations error

#2 Insider attacks

#1 User Error

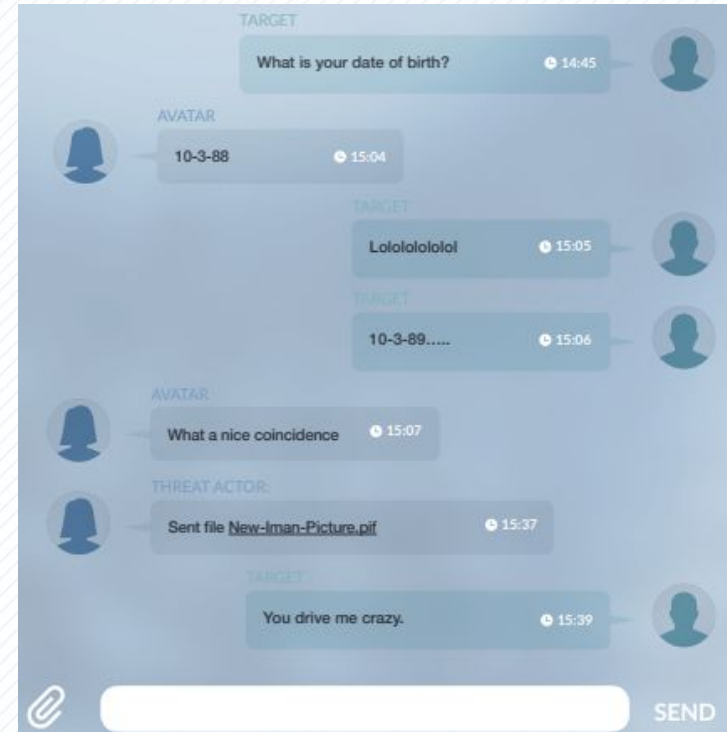


# #5 Social Engineering

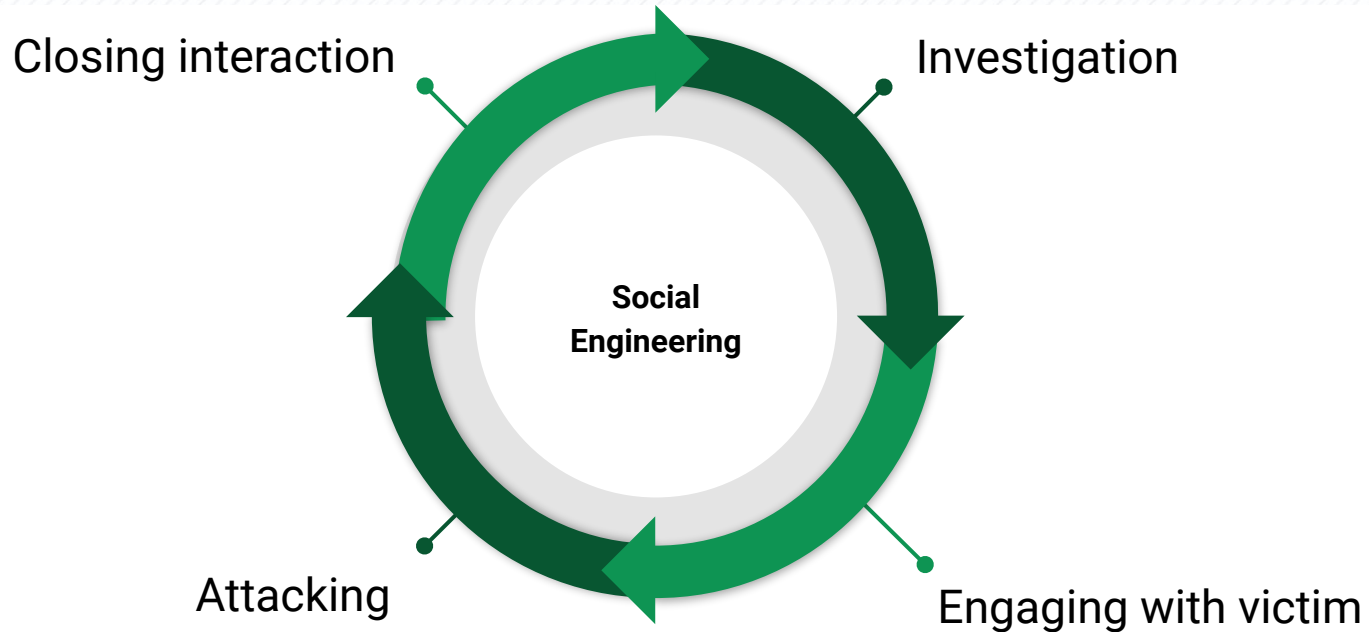
# Social engineering

2013, Syrian opposition forces and humanitarians targeted via Skype. Stolen data included:

- » Humanitarian needs assessments
- » Lists of materials for the construction of major refugee camps
- » Humanitarian financial assistance disbursement records



# Social Engineering



# Phishing

- Attackers impersonate legitimate businesses
- Urgency created by presenting consequences
- Rely on spamming large groups



# Spear-Phishing

- Sophisticated form of phishing
- Extensive research to the target
- Impersonating a trusted partner



# Whaling/CEO-Fraud

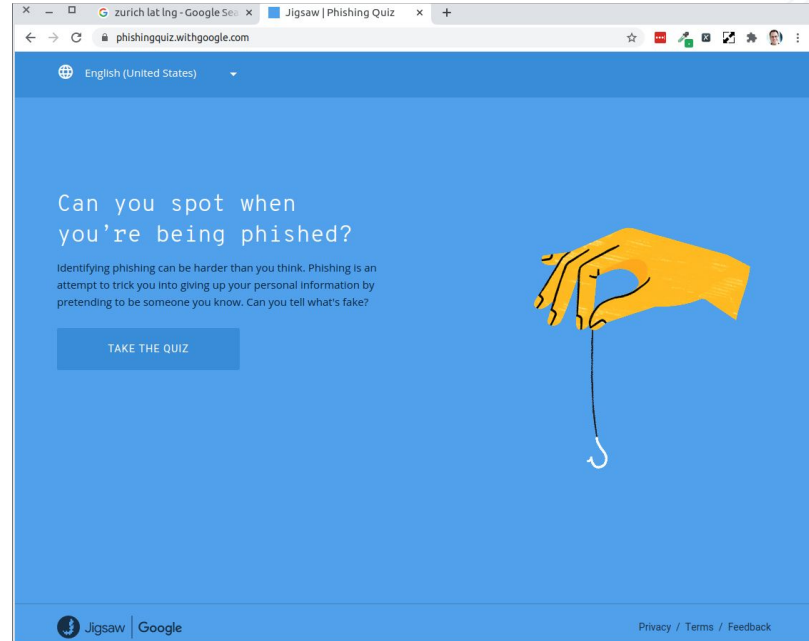
- Spear-phishing on high level position
- Using the authority of the “whale”



## MITIGATION

# Social Engineering

- Training and awareness
- Check the sources!
- Don't rush it!



# #4 Password management

# Weak & reused passwords

Use of default admin password allowed competitor of RedRose to access more than 8,000 names, photos, family details and map coordinates of beneficiaries in West Africa.



# Passwords: the basics

- No more recycling
- Use two factor authentication when possible
- Use a password manager

Visit <https://haveibeenpwned.com/>

Massive data breaches mean that your go-to password may be out there in the world.



# Password Manager

- Only one password to remember
- Automatically generated passwords
- Notify when it's time to change

Password managers:

- LastPass
- 1-password
- Default browser manager (Chrome/Firefox)



# Migrate to SSO

**Single-Sign on via your organization significantly reduces risk of Account Takeover Attacks (ATO) *and* Insider attacks.**

- Enforce organization-level policies on 2FA, device security
- Eliminate sloppy passwords
- Inherit organization-level account security
- Ex-employees automatically blocked



# Enabling SSO in ActivityInfo

**ActivityInfo** Search for a database, folder ... Databases Reports

**Account settings**

**Profile settings**

Billing account

API Tokens

Offline storage

**Profile settings**

Your name

testing

Preferred language

English

LOGGED IN AS  
testing  
qa@bedatadriven.com

Logout

Profile settings

Billing account

Switch language

Version 4.0 Build 1278

✕ Cancel ✓ Save profile

**Secure your account**

You are currently logging in with an ActivityInfo password. To improve the security of your account, we recommend that you enable Single-Sign On.

Connect your Google account



#3

# IT Operations Failures

# IT operations failures

Allowing Domains or Accounts to Expire • Buffer Overflow • Business logic vulnerability • CRLF Injection • CSV Injection • Catch NullPointerException • Covert storage channel • Deserialization of untrusted data • Directory Restriction Error • Doubly freeing memory • Empty String Password • Expression Language Injection • Full Trust CLR Verification issue Exploiting Passing Reference Types by Reference • Heartbleed Bug • Improper Data Validation • Improper pointer subtraction • Information exposure through query strings in url • Injection problem • Insecure Compiler Optimization • Insecure Randomness • Insecure Temporary File • Insecure Third Party Domain Access • Insecure Transport • Insufficient Entropy • Insufficient Session-ID Length • Least Privilege Violation • Memory leak • Missing Error Handling • Missing XML Validation • Multiple admin levels • Null Dereference • Overly Permissive Regular Expression • PRNG Seed Error • Password Management Hardcoded Password • Password Plaintext Storage • Remote code execution • Return Inside Finally Block • Session Variable Overloading • String Termination Error • Unchecked Error Condition • Unchecked Return Value Missing Check against Null • Undefined Behavior • Unreleased Resource • Unrestricted File Upload • Unsafe JNI • Unsafe Mobile Code • Unsafe function call from a signal handler • Unsafe use of Reflection • Use of Obsolete Methods • Use of hard-coded password • Using a broken or risky cryptographic algorithm • Using freed memory • Vulnerability template • XML External Entity (XXE) Processing • SSL misconfiguration

# IT operations failures

400 GB of data was stolen from UN servers in 2019

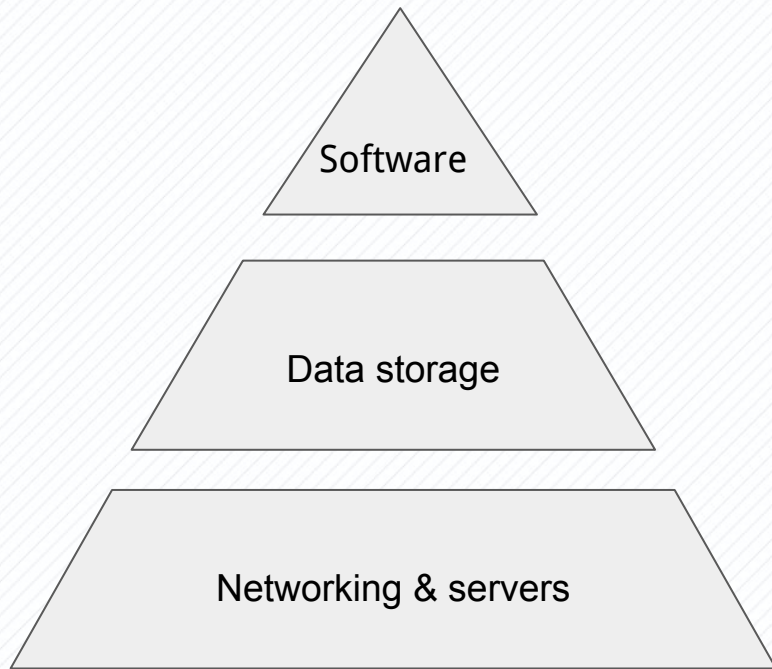
**Feb 2019:** Alert for bug in Sharepoint published

**July 2019:** Attackers exploited this bug to gain access to UN systems



## MITIGATION

# IT operations failures - specialization



ActivityInfo



Google Cloud  
Datastore



#2

# Insider Attacks

# Insider attacks

In 2005, a local NGO staff member was fired, and using his credentials, deleted all his NGO's reports in ActivityInfo.



# Insider attacks

- Threats from within your own company
- Difficult to deal with
- Three types of insider threats



# Insider attacks: The malicious user

- Bad actor in organization
- Emotionally motivated



## MITIGATION

# Insider attacks

- Narrow user permissions
- Data-loss prevention measures



Database design

User management

Roles

Audit log

## Audit log

Events before 2020-07-14 11:26 Filter by event type Filter by form or folder

- 2020-07-14 10:56 — FAY  
Added a record in Deliveries
- 2020-07-14 10:37 — FAY  
Deleted a record in Monitoring for Education programmes  
[Recover record](#)
- 2020-07-14 10:37 — FAY  
Added a record in Monitoring for Education programmes
- 2020-07-14 10:25 — FAY  
Recovered a deleted record in Deliveries
- 2020-07-14 10:12 — FAY  
Updated a record in Monitoring for Education programmes
- 2020-07-14 10:11 — FAY  
Added a record in Monitoring for Education programmes
- 2020-07-14 10:11 — FAY  
Deleted a record in Deliveries [Reverted](#)
- 2020-07-14 10:11 — FAY  
Added a record in Weekly deliveries in Deliveries

## Updated a record in Monitoring.

TIME  
2020-07-14 10:12

USER

Fay

FORM

[Monitoring for Education programmes](#)

### Record history

2020-07-14 10:12:00 AM  
Record edited

FAY — FAY@E

SELECT THE PROGRAMME YOU REPORT FOR:  
Blank → Education for Adults 2020

2020-07-14 10:11:51 AM  
Record added

FAY — FAY@BI

#1

User Error

# User error

“An email holding the private data of 8,253 users enrolled onto courses on immunisation went out to around 20,000 Agora users in late August [2019]”

“This was an inadvertent data leak caused by an error when an internal user ran a report...”



## MITIGATION

# User error

## Narrow user permissions

Consider whether users really need the ability to **Edit** or **Delete**.

For sensitive data, be careful with **Export** and **Publish** permissions.



The screenshot shows the 'Permissions' tab of a user configuration interface. It lists various permissions with checkboxes, some of which are selected. The 'Parameters' tab is also visible at the top right.

Permissions	Parameters
<b>Edit permissions</b>	
<input type="checkbox"/> View all records	
<input checked="" type="checkbox"/> View where partner is user's partner	
<input type="checkbox"/> Add any record	
<input checked="" type="checkbox"/> Add records where partner is user's partner	
<input type="checkbox"/> Edit all records	
<input checked="" type="checkbox"/> Edit records where partner is user's partner	
<input type="checkbox"/> Delete any record	
<input checked="" type="checkbox"/> Delete records where partner is user's partner	
<input checked="" type="checkbox"/> Export records	
<input type="checkbox"/> Manage users	
<input type="checkbox"/> Manage record locks	
<input type="checkbox"/> Add forms and folders	
<input type="checkbox"/> Edit forms and folders	
<input type="checkbox"/> Delete forms and folders	
<input type="checkbox"/> Share reports	
<input type="checkbox"/> Publish reports	

Buttons:

## Narrow user permissions

We analysed each of our customers, and between

**40 - 75%**

of users *granted* administrative privileges are *not using* them



# Narrow roles

DATABASES > ACTIVITY 4: WINTERIZATION KITS 2020 > DATABASE SETTINGS

**Database settings**

Database design

User management

**Roles**

- SL Sector Lead
- A Administrator
- RP Reporting partner

**No role selected**

Click on a role to see the related permissions.

# Risk-management: we can do this!

- NGOs have lots of experience with risk management
- We need to view data security through the same lens:
  - What are the risks?
  - How much risk do we accept?
  - How do we mitigate risks?

# *Questions?*

## Social media

Twitter: [@activityinfo](https://twitter.com/activityinfo)

LinkedIn:

<https://www.linkedin.com/showcase/activityinfo>

### **NEXT WEBINAR**

"A guide to choosing sample sizes for M&E practitioners"

May 27, 15:00 CEST

Register at:  
<https://www.activityinfo.org/>