OASIS

CyberDetective

COMIC PART 2 OF 6

PART 2/6

Welcome to the World of Oasis where its inhabitants are kept safe by the technology they surround themselves with as they try to rebuild their lives. In this episode the detective has to meet her old acquaintance.

Chief Editor &
Transmedial Producer:
Vincent "South-Blessed" Baidoo
Artist: Connor Rawlings
Front Cover: Jonathan Tonello
Writer: Vincent Baidoo
Editor: Niki Baidoo
Writer & Researcher: Patrick Shortis
Extra Art: Vladimir Rikowski, Francisco Ruiz
Special Thanks: Jeremy Charles, Tomas Hall

CyBOK

CROWNROOT publications

University of BRISTOL

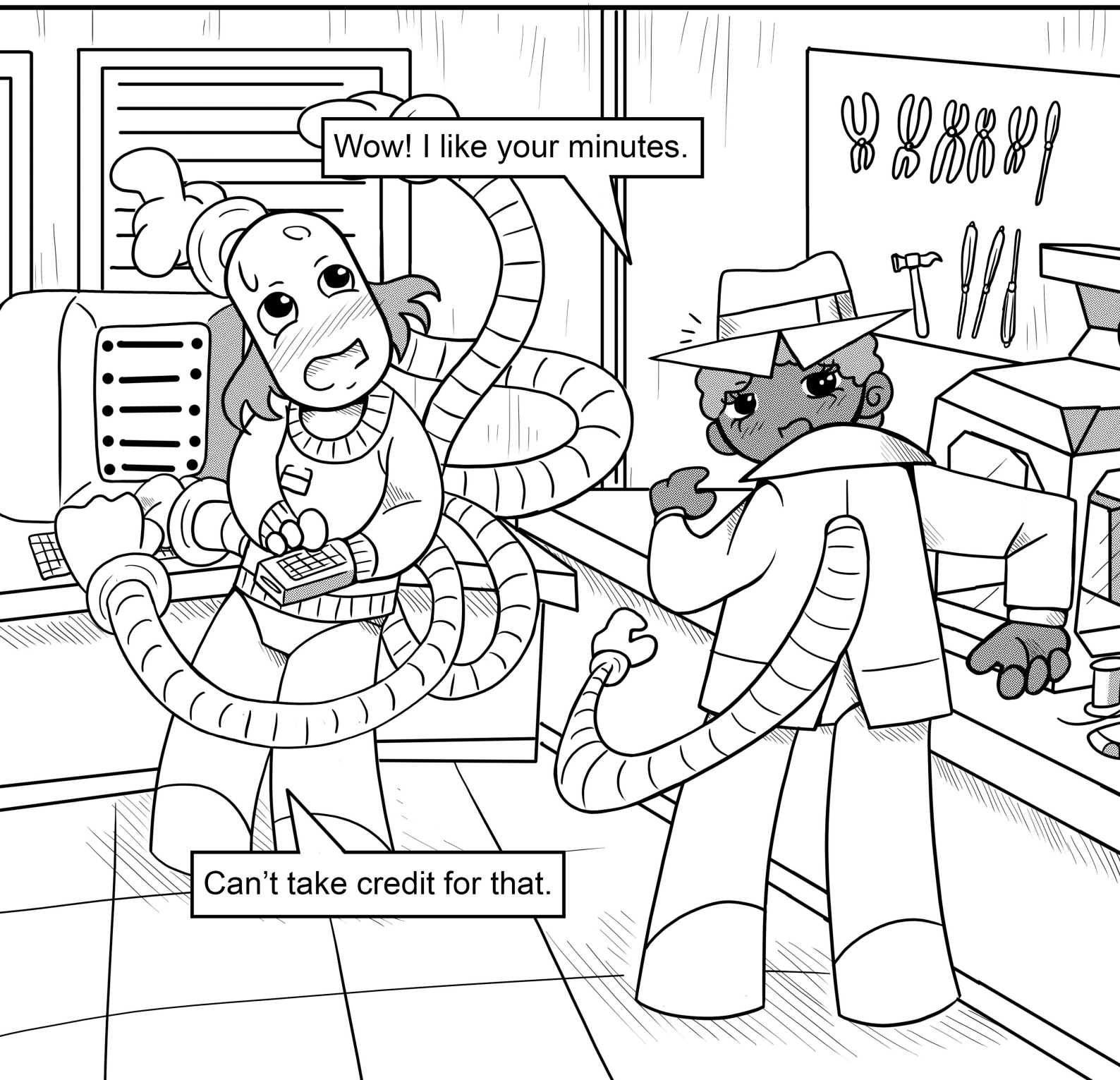
UKRI Research England

THIS PUBLICATION IS A RESULT OF CYBOK AND CROWNROOT PUBLICATIONS FUNDED BY BRISTOL UNIVERSITY AND RESEARCH ENGLAND

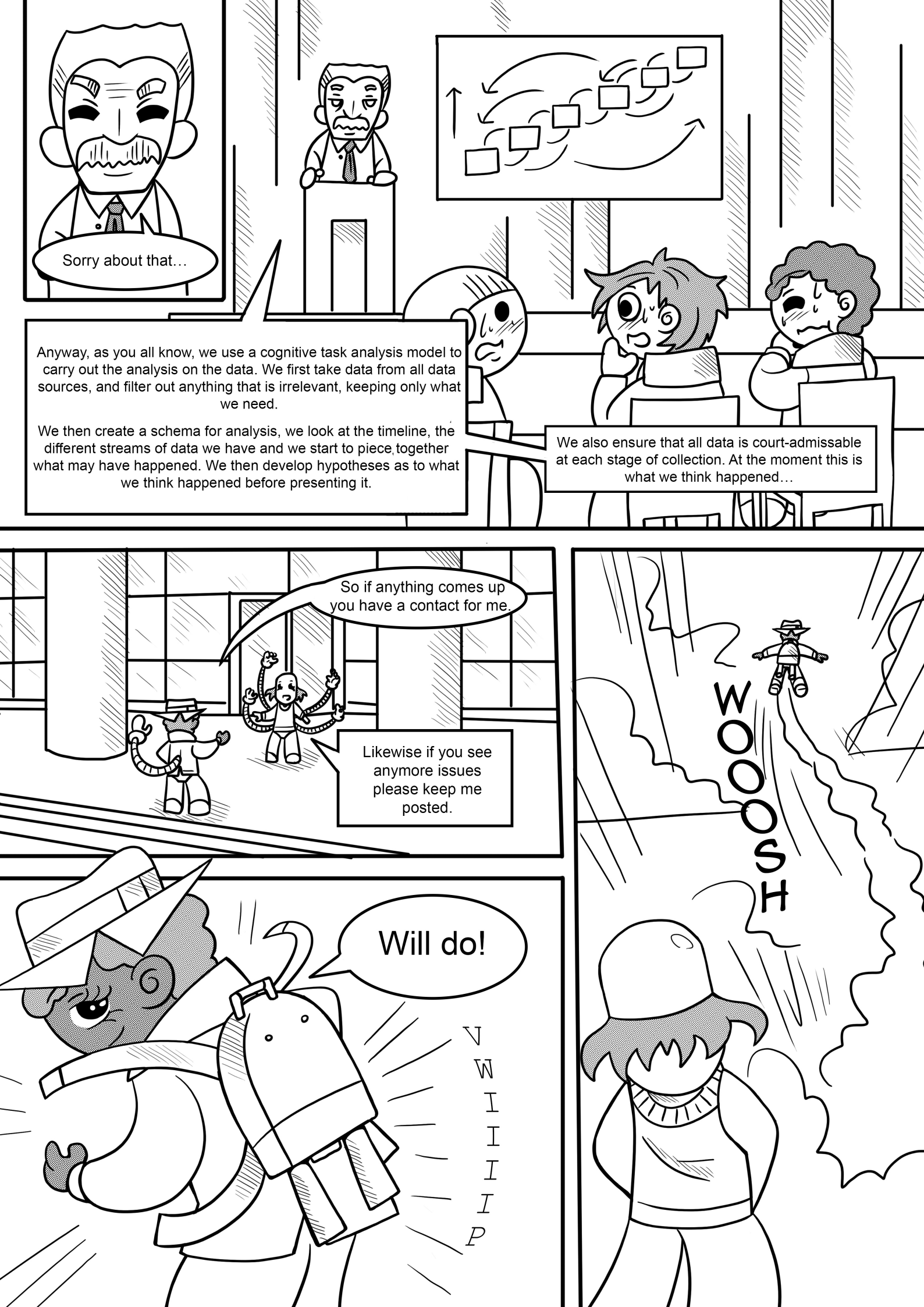
So what we just gonna stand here and wait?

I'm doing loads with my hands...

Generators will come on if you give me a minute.



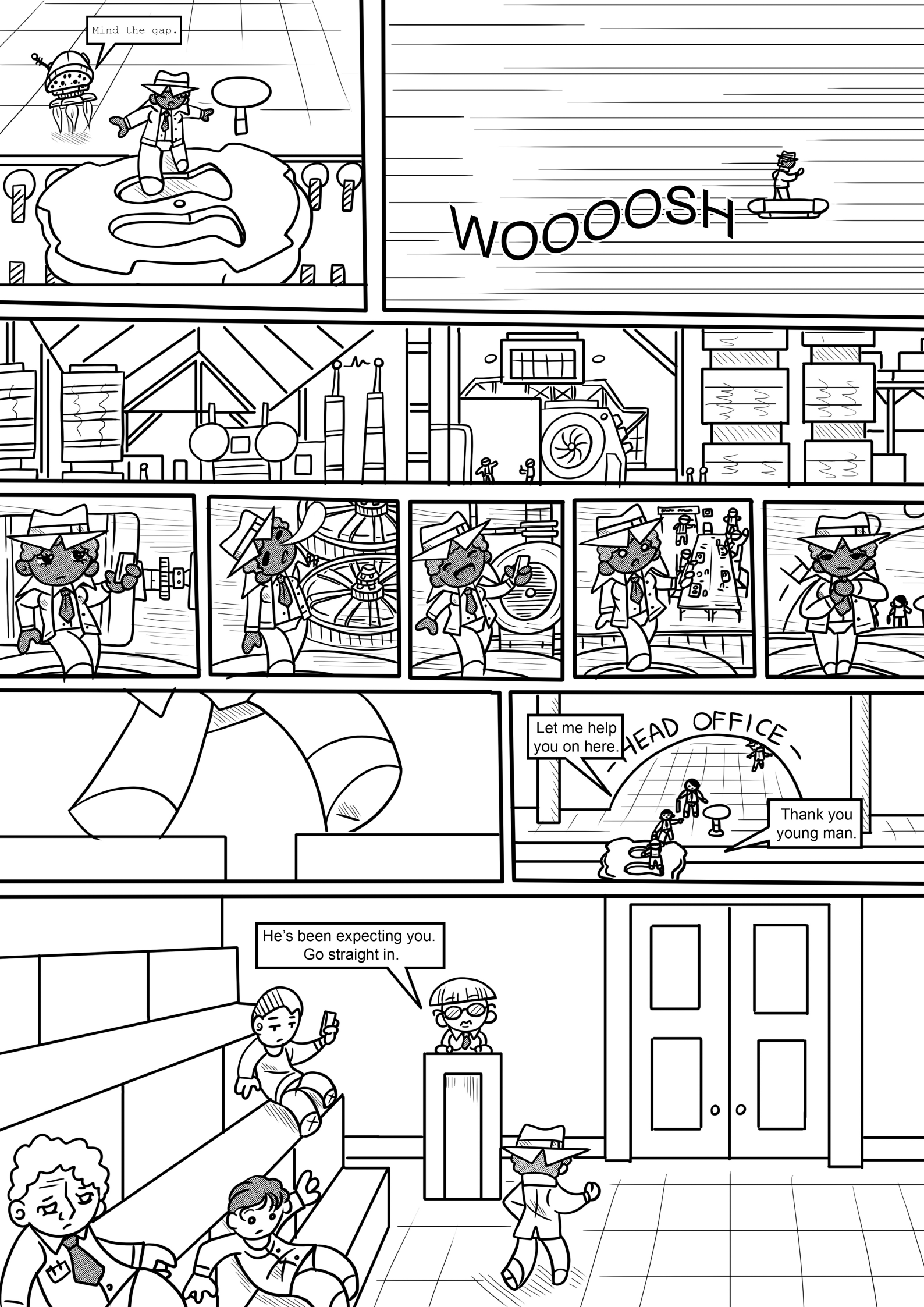

Looks like the grid's back up!
Looks like it…
RING
RING
RING
So I take it the candles weren't just blown out over here then?
Quit messing about and get to the power plant...NOW!
Lucky the Juniors weren't around to hear that.
Yeah real lucky!!

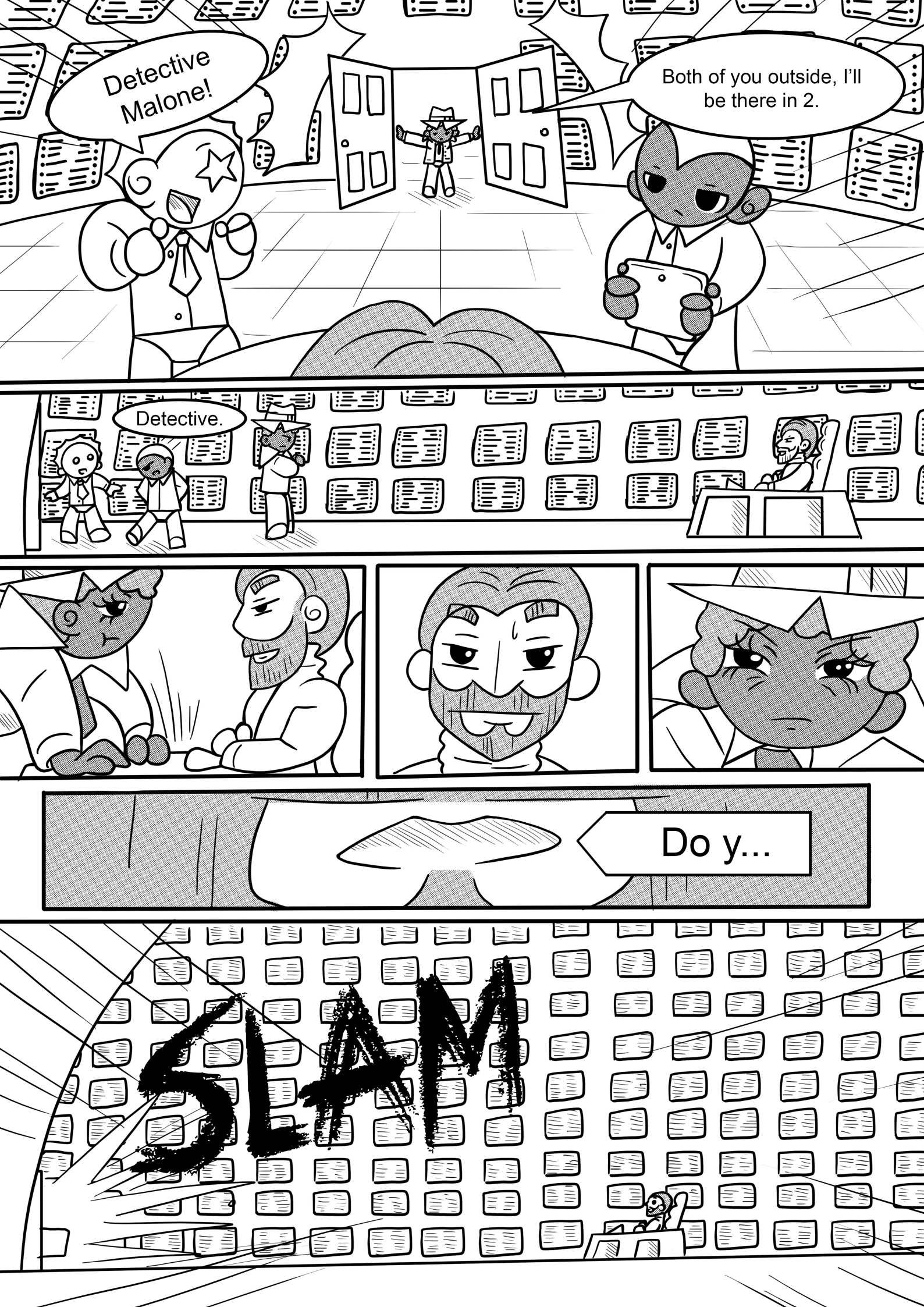

Sorry about that…
Anyway, as you all know, we use a cognitive task analysis model to carry out the analysis on the data. We first take data from all data sources, and filter out anything that is irrelevant, keeping only what we need.
We then create a schema for analysis, we look at the timeline, the different streams of data we have and we start to piece together what may have happened. We then develop hypotheses as to what we think happened before presenting it.
We also ensure that all data is court-admissable at each stage of collection. At the moment this is what we think happened…
So if anything comes up you have a contact for me.
Likewise if you see anymore issues please keep me posted.
WOOOSH
Will do!
VWIIIIP

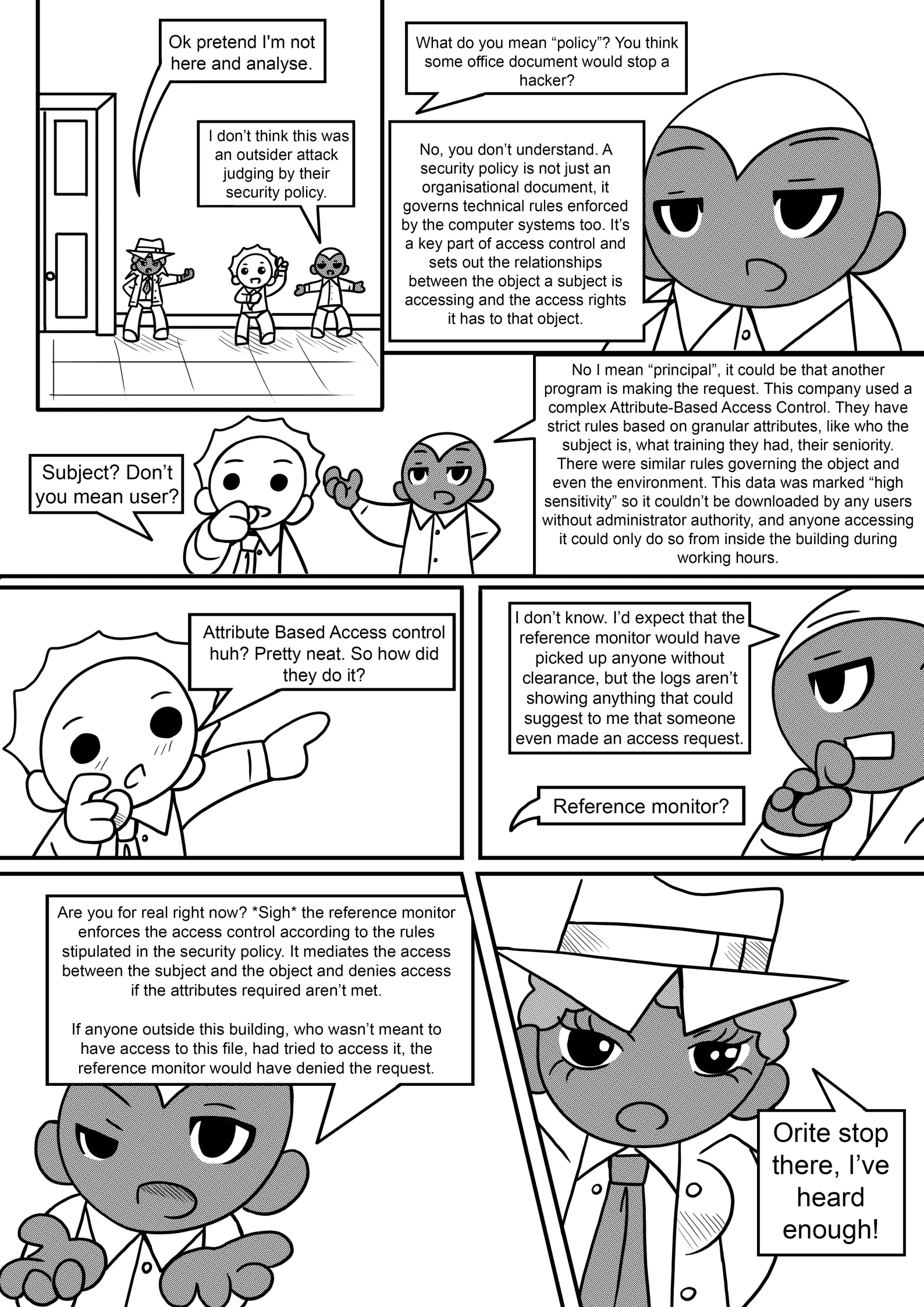

I need to not let my emotions make me miss any details.
Let me do my best to not stir things up.
How very elegant of you to notice the entrance!
How very observant of you to notice an entrance…
...your job must be so tiring!


HUFF
It's going to be a little slower than your jetpack but we'll get there…
It's not that slow.
Head office I take it?
Head office thank you…


It's nice in here!
Ok you win, that was too fast!
Do that again and I'm going to have to write you a ticket.
Safe travels detective.


Mind the gap.
WOOOOSH
Let me help you on here.
HEAD OFFICE
Thank you young man.
He's been expecting you. Go straight in.


Detective Malone!
Both of you outside, I'll be there in 2.
Detective.
Do y...
LAM


Ok pretend I'm not here and analyse.
I don't think this was an outsider attack judging by their security policy.
What do you mean "policy"? You think some office document would stop a hacker?
No, you don't understand. A security policy is not just an organisational document, it governs technical rules enforced by the computer systems too. It's a key part of access control and sets out the relationships between the object a subject is accessing and the access rights it has to that object.
Subject? Don't you mean user?
No I mean "principal", it could be that another program is making the request. This company used a complex Attribute-Based Access Control. They have strict rules based on granular attributes, like who the subject is, what training they had, their seniority. There were similar rules governing the object and even the environment. This data was marked "high sensitivity" so it couldn't be downloaded by any users without administrator authority, and anyone accessing it could only do so from inside the building during working hours.
Attribute Based Access control huh? Pretty neat. So how did they do it?
I don't know. I'd expect that the reference monitor would have picked up anyone without clearance, but the logs aren't showing anything that could suggest to me that someone even made an access request.
Reference monitor?
Are you for real right now? *Sigh* the reference monitor enforces the access control according to the rules stipulated in the security policy. It mediates the access between the subject and the object and denies access if the attributes required aren't met.
If anyone outside this building, who wasn't meant to have access to this file, had tried to access it, the reference monitor would have denied the request.
Orite stop there, I've heard enough!


What do you have for me directly?
Give...me...2 seconds and...I'll...have...
BEEP
...Everything transcribed for you!
Endeavour formally acknowledged.
Ok let's cut the sweety talk and get straight to it... what's happened here?
What is "Sweety" talk?
WHY WAS THERE A BLACK OUT? ...GO!


Do you know what happens when 72% of this region decide to put their coolers on max…
A REGION BLACKOUT THAT'S WHAT!!
How about we both calm down and deal with this a little more efficiently...so what is it you're saying? That the black out wasn't the energy plant's fault? So you have been attacked?...
...just asking you to bring me up to speed...walk me through it
I woke up this morning and my temperature was set to high, as I was changing the settings I get a message from Management saying I've been doxed and to come in...
We'll get to the doxing but could you stay on the Energy... please continue.
Do you know we carry out a lot of data analysis on users in the region so that we can think more carefully about matching services to them. Things like age, postcode, salary etc.
That sounds like a major privacy concern if an attacker can find a lot of information on them.


We do a lot of work to delink the data points to the users so they can't be matched. We first anonymise the data and remove anything that would be an obvious link to a person's identity, like their name. We then generalise the data to reduce its accuracy.
Area codes are reduced to the first two numbers so we know which district they live in, but not which street. Similarly their ages are generalised from "27" to "20-30". It means the data is too general to point to any one person.
Politely I'm asking can you get to the point...
The point is, when I came in, the investigation into the doxing highlighted a surge of energy usage caused by the users themselves but because of our own Data Obfuscation we didn't have specific details.
We decided to send a mass email to everyone to check their setting, look for mistakes, pre-empted frequently asked questions and things of this nature, 3 and a half minutes after we sent the email the blackout happened.
Did people take the message the wrong way? Did you use too technical language or something?
Do you know how good our writing team is! No it turns out as soon as we sent our email 2-4 emails were sent appearing to come from our email address stating exactly the opposite of what we wanted.
Pollution attack huh, so this confirms this is actually an attack. What exactly did it say?
I'll send it to you now, but basically it stated "we're about to have a heat wave so put your coolers on max."
Interesting...and so your temperature being set too high, is that part of this? did that happen to everybody else?
We don't know, nothing came up on our system.
K...couple basic questions...anyone ever upload something that could compromise the system?
When a user uploads a file on our system we scan it for malware and have several restrictions in place governing both the metadata of the file and the content of the file.
Malware and other undesirables are scanned for, filtered out and the IP address of the culprit is logged and banned from reconnecting. We also use a separate domain so that any file that does make it through doesn't have access to any cookies and other information on the domain from where we serve content.


Sounds absolutely perfect...next question: have you been on any dodgy websites?
What!?
You heard what I said.
Do you know?…
Get your spam folder up.
So clearly you're a frequent user of Psychic Readings.com.
I don't know what this has to do with anything…
For crying out loud Archibald... You got done by a basic phishing attack...
...You two come in for a second.
What's going on?
This email here you clicked it right?

How can we help?

I'm going to send you a link I need you to give it a full once over.

Look the link in this email goes to this site...this is the site you usually go onto right?

*Sigh...I know what a phishing attack is Victoria...

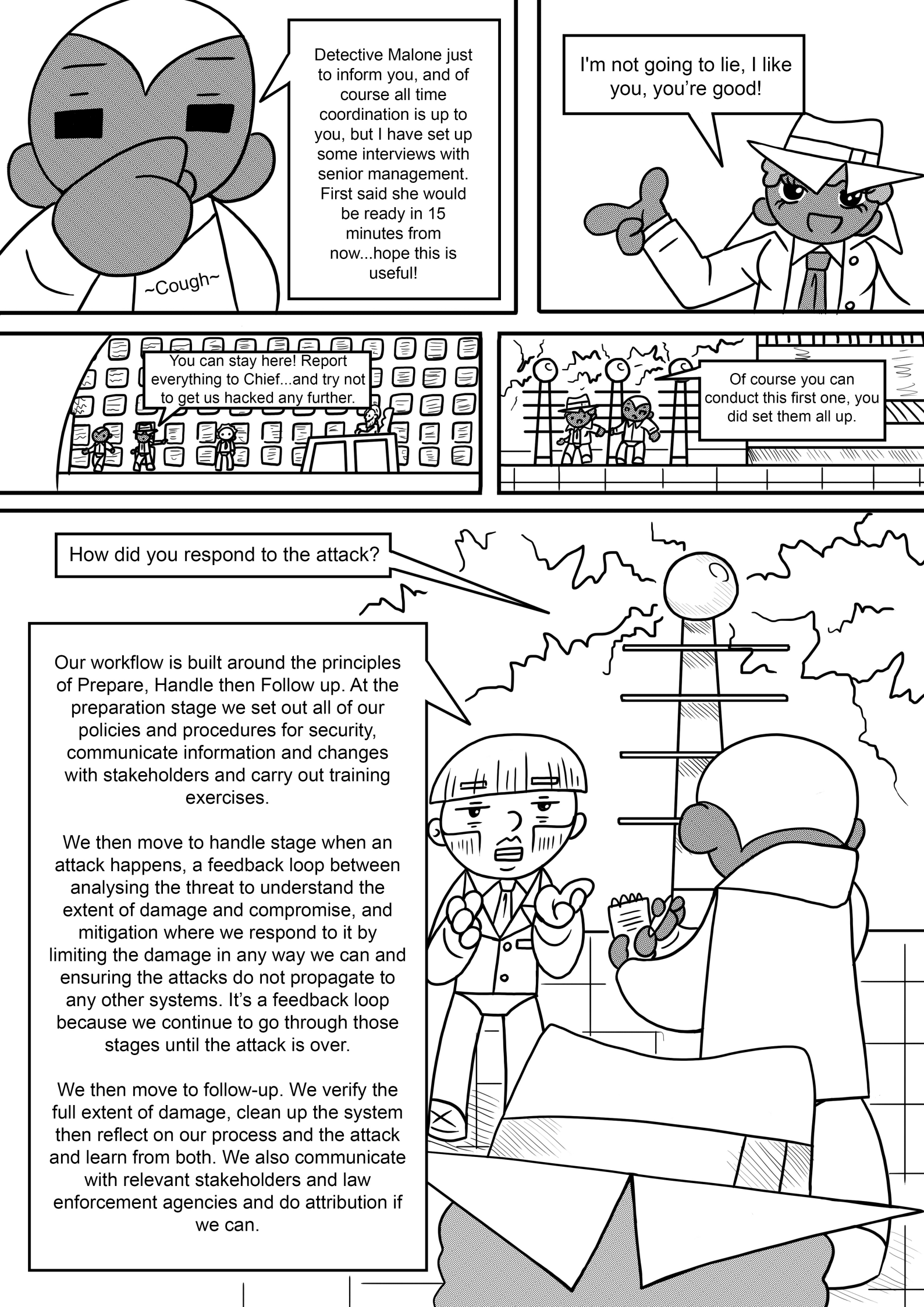
www.qsychicreadings.com

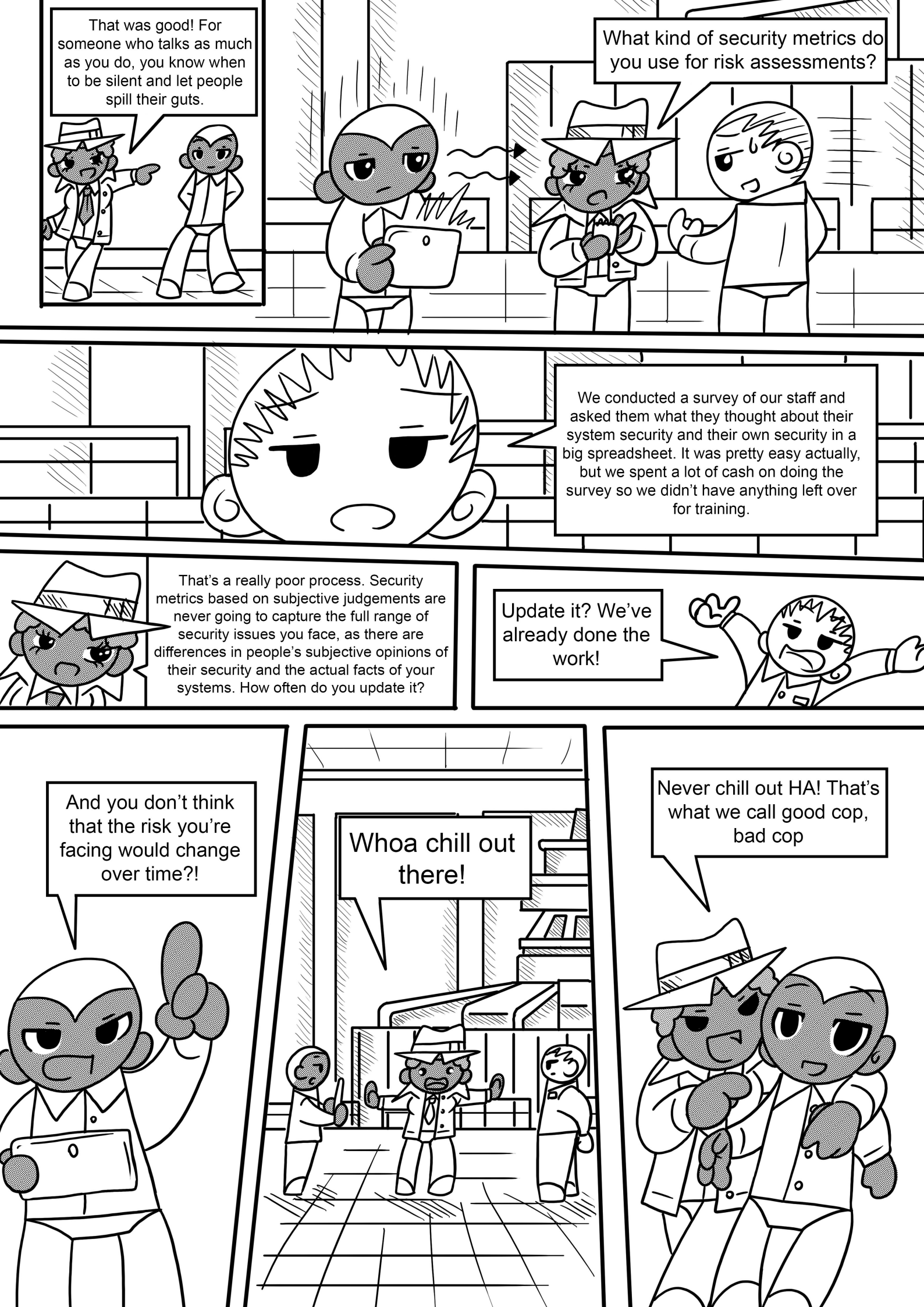
WRONG! This is not the same site, look closely you can see it's spelt with a "q" not a "p". So whatever information you entered into this session will have most likely gone somewhere for malicious use.

Detective Malone quick question, where is the doxed information being held? Can't we just shut off the server?

No you can't... It's not just one machine; It's distributed across the entire web. That'd be like turning off the whole internet. The best thing you can do now is speak to your bank and fraud prevention services to help protect yourself and replace any IDs that may have been stolen.

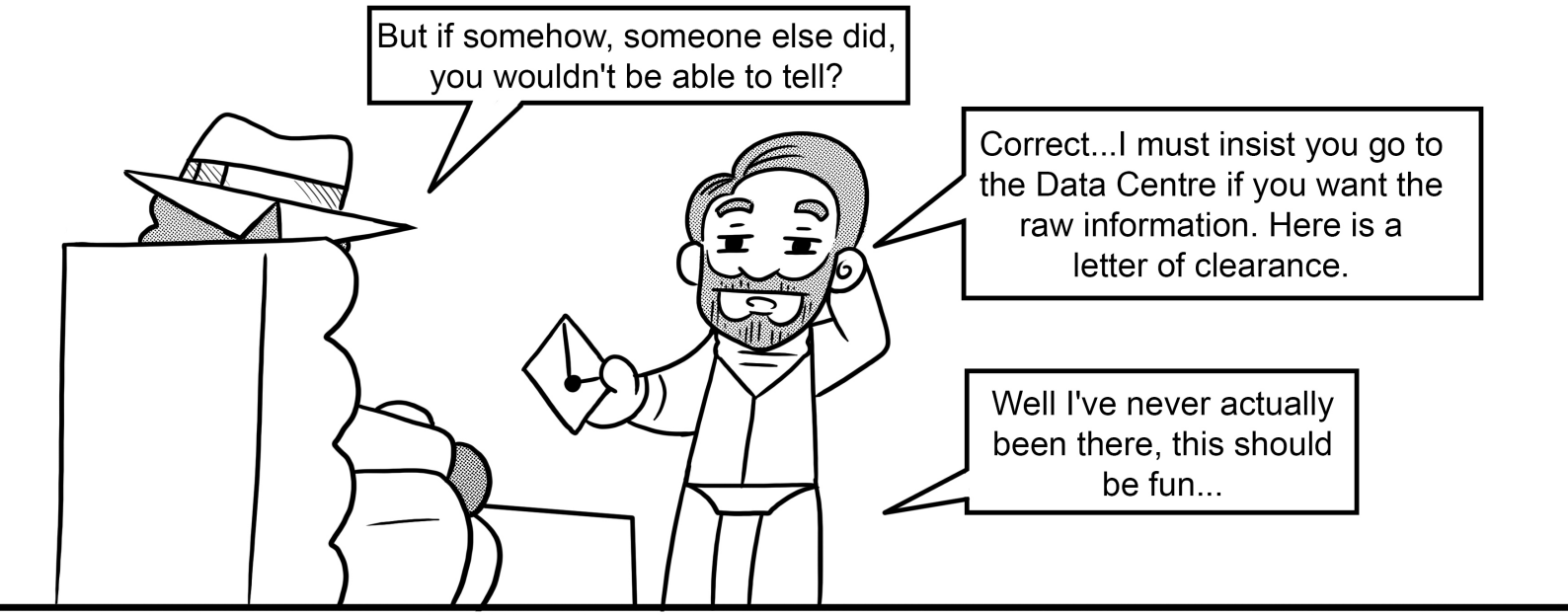

Ok preliminary scans on phishing email complete...
Now to examine the link.
WHAT ARE YOU DOING?!
I was going to open it-
On your own operating system? Use a virtual machine!
But that takes up resources on the computer!
Yes but hardened sandboxes like Qubes OS, isolate and compartmentalise computer resources so it is harder for malware to get a foothold in the system. The malware would need to compromise the sandbox itself before it could find data hidden in other containers.
Please PLEASE remember this for next time, very VERY serious mistake you nearly made there.
I can think of at least 7 reasons why none of this should be funny to you.

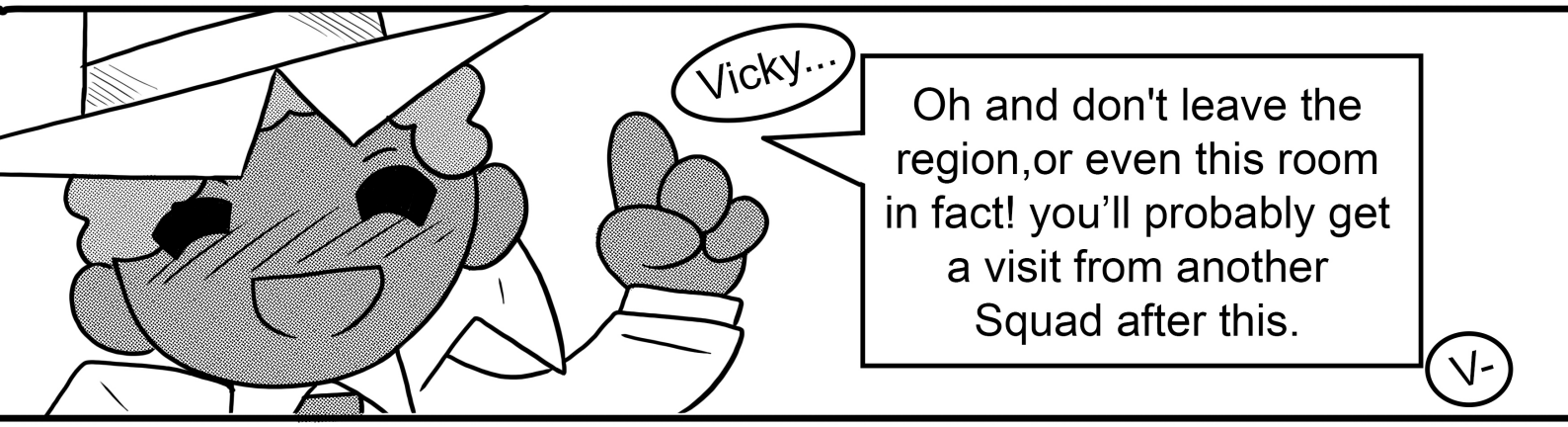

~Cough~
Detective Malone just to inform you, and of course all time coordination is up to you, but I have set up some interviews with senior management. First said she would be ready in 15 minutes from now...hope this is useful!
I'm not going to lie, I like you, you're good!
You can stay here! Report everything to Chief...and try not to get us hacked any further.
Of course you can conduct this first one, you did set them all up.
How did you respond to the attack?
Our workflow is built around the principles of Prepare, Handle then Follow up. At the preparation stage we set out all of our policies and procedures for security, communicate information and changes with stakeholders and carry out training exercises.
We then move to handle stage when an attack happens, a feedback loop between analysing the threat to understand the extent of damage and compromise, and mitigation where we respond to it by limiting the damage in any way we can and ensuring the attacks do not propagate to any other systems. It's a feedback loop because we continue to go through those stages until the attack is over.
We then move to follow-up. We verify the full extent of damage, clean up the system then reflect on our process and the attack and learn from both. We also communicate with relevant stakeholders and law enforcement agencies and do attribution if we can.

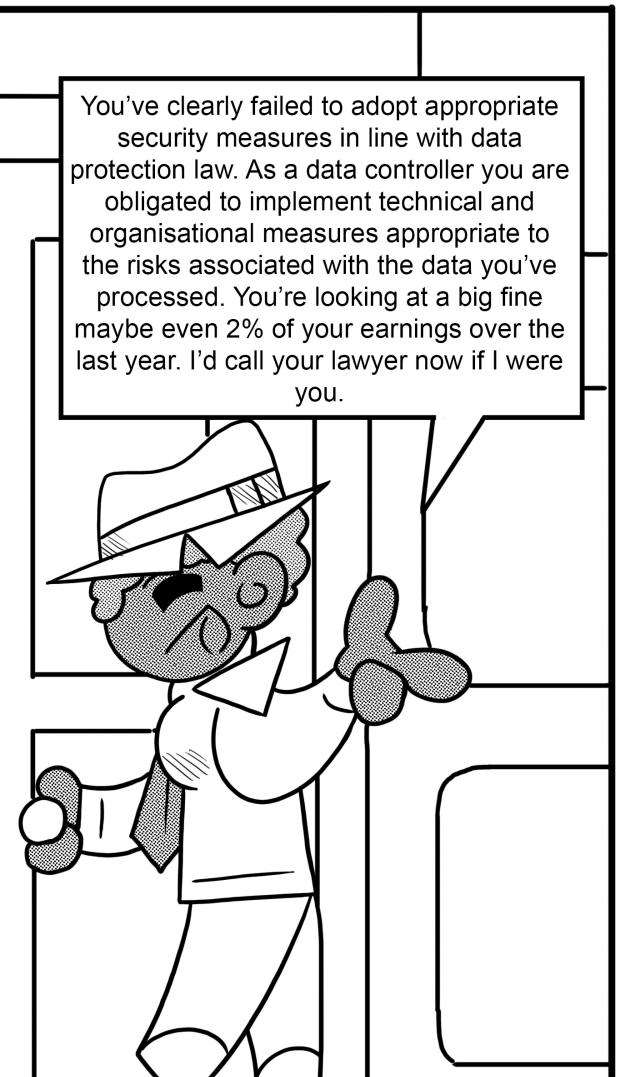

That was good! For someone who talks as much as you do, you know when to be silent and let people spill their guts.
What kind of security metrics do you use for risk assessments?
We conducted a survey of our staff and asked them what they thought about their system security and their own security in a big spreadsheet. It was pretty easy actually, but we spent a lot of cash on doing the survey so we didn't have anything left over for training.
That's a really poor process. Security metrics based on subjective judgements are never going to capture the full range of security issues you face, as there are differences in people's subjective opinions of their security and the actual facts of your systems. How often do you update it?
Update it? We've already done the work!
And you don't think that the risk you're facing would change over time?!
Whoa chill out there!
Never chill out HA! That's what we call good cop, bad cop

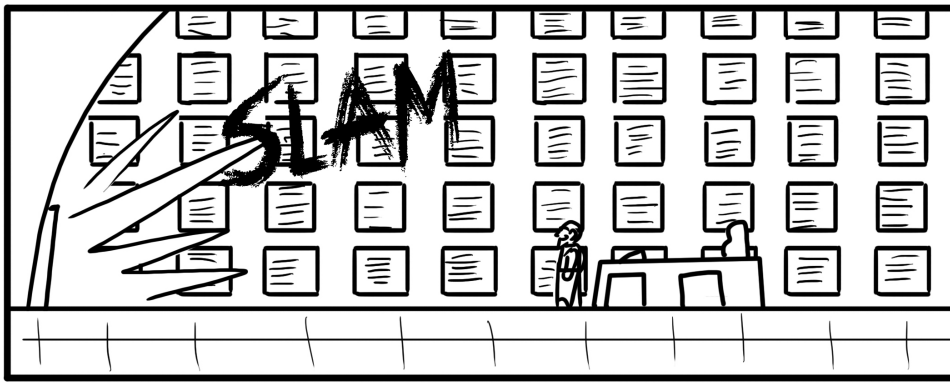

Don’t you train your staff regarding cyber risks that they have a part in?
Like what?
Making sure that they use password managers, training them what phishing emails and other attacks might look like and using a browser that exposes deceptive URLs. You know - the bare MINIMUM a company like yours should do.
Come on, we’ve never been attacked before. Those kind of training costs are overheads that our bosses don’t want to pay for. We have policies in place regarding password length, rules against using our work computers for visiting certain sites, but nobody takes them seriously.
You should be putting in place much more rigorous risk assessments and training, communicate them to your staff, and get them to understand their role in protecting your company.
Sorry Detective Malone.
I think Mr Baylies has something important to tell you.
You two wait outside I'll be a sec.
Do you know…


...how good it's been seeing you again?
Archie…
...that is not what you called me here to say.
There is a backdoor in the system we know about.
Ok I'm going to take a seat.
Back when this organisation got full backing to be sole energy supplier, that very season we had a freak cool period.
Cool only in temperature.
Well calculations were done and it was predicted that if the cool period become even a semi permanent or periodical circumstance then profits would plummet, and as you know up until very recently we were the highest grossing company in Oasis.
I'm really not going to like this am I?
If we went down then our whole economic situation was fudged...so we implemented a way to increase temperatures and it not show up on our main systems here.
Don't tell me this was the real reason for all your walk outs?
It didn't help…
The cool spell left and never came back as you know, and we have never used the backdoor again.


But if somehow, someone else did, you wouldn't be able to tell?
Correct...I must insist you go to the Data Centre if you want the raw information. Here is a letter of clearance.
Well I've never actually been there, this should be fun...


Vicky...
Oh and don't leave the region,or even this room in fact! you'll probably get a visit from another Squad after this.
V-


You've clearly failed to adopt appropriate security measures in line with data protection law. As a data controller you are obligated to implement technical and organisational measures appropriate to the risks associated with the data you've processed. You're looking at a big fine maybe even 2% of your earnings over the last year. I'd call your lawyer now if I were you.


SLAM


Chief...you there? ...ok listen...they're putting pork in the vegan cream if you get what i'm saying.
Well that's pretty sticky.


Yeah, thickens the plot for sure, will give an encrypted voice note to one of the Juniors with all the info for you.
Wouldn't it be safer to pop back, probably about time you took a break!
I can trust one of the guys you sent here, pretty decent all round if I'm honest, but I'll code up the wording anyway.
Well Psychic Readings.com, is in compliance with lawful interception laws.
Ah, so they're compelled to procure and maintain facilities designed to facilitate the lawful interception of communications that traverse their domain.
Yeah the hackers may have had no interaction with their official site but we will get a warrant and we might get a lead from them.
Sounds good…One sec Chief got another call… Hello Bart! What's up?
Detective I got something to tell you that I should've done earlier...
Not you as well...
TBC