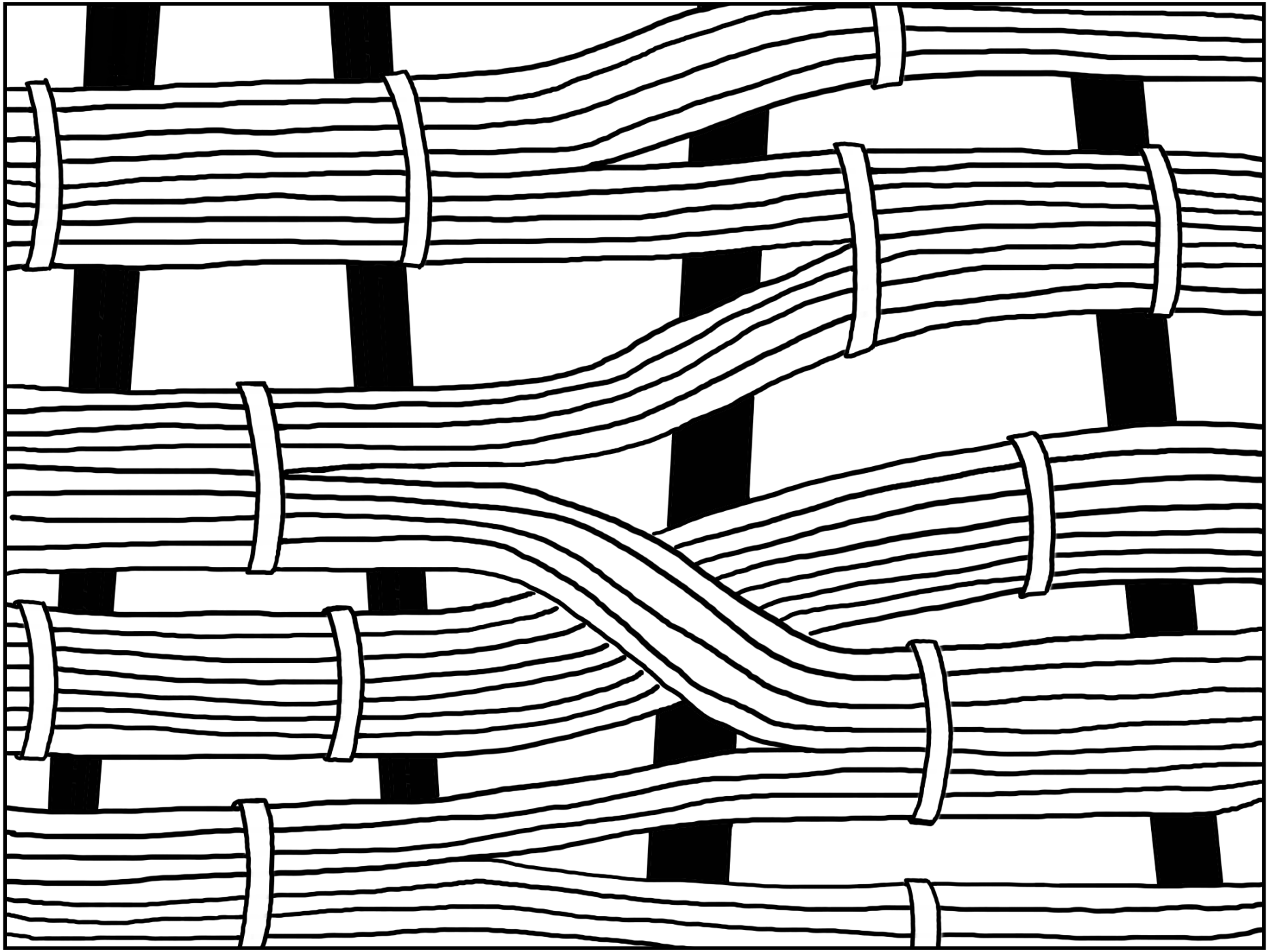

ADVANCED ENDPOINT PROTECTION: SECURING THE MEATY BITS
mindful tips for people who care about security

You care about security, right? And you want to do everything you can to look after your information system.

Security practitioners have to be generalists. We need to understand what the systems we're protecting are made of, and a little bit about how all the parts work.

So what's yours made of?

Spinning disks and circuit boards? Cables and radio waves? Code repositories and clouds?



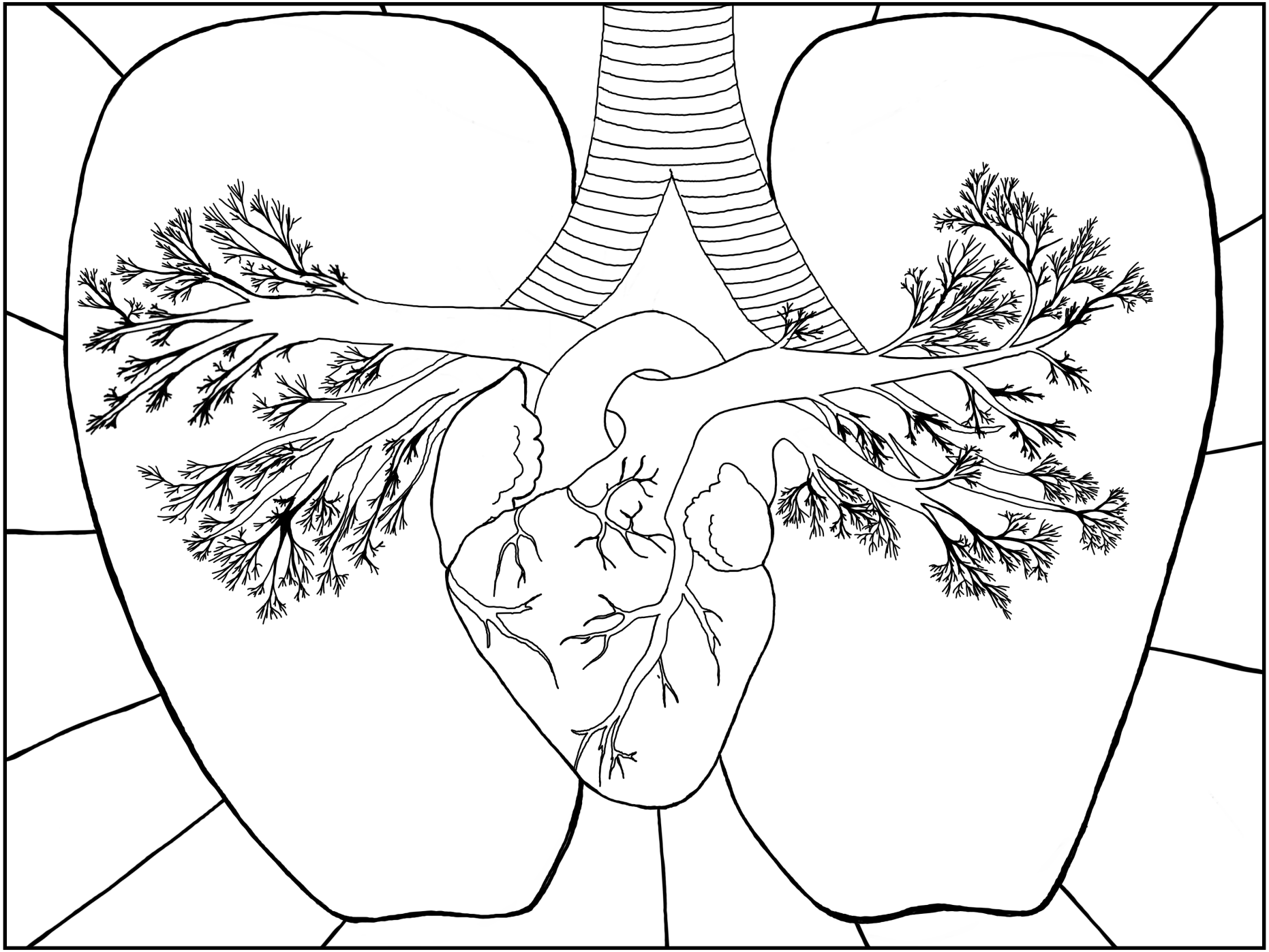
Something's missing from our network diagrams. Information systems are more than plastic, copper and silicon.

They're mostly made out of people.

Information systems are made *by* people, *for* people to do things *with* people and *for* people.

And for our system to be secure, all these people need to be protected.

So how do we do that?



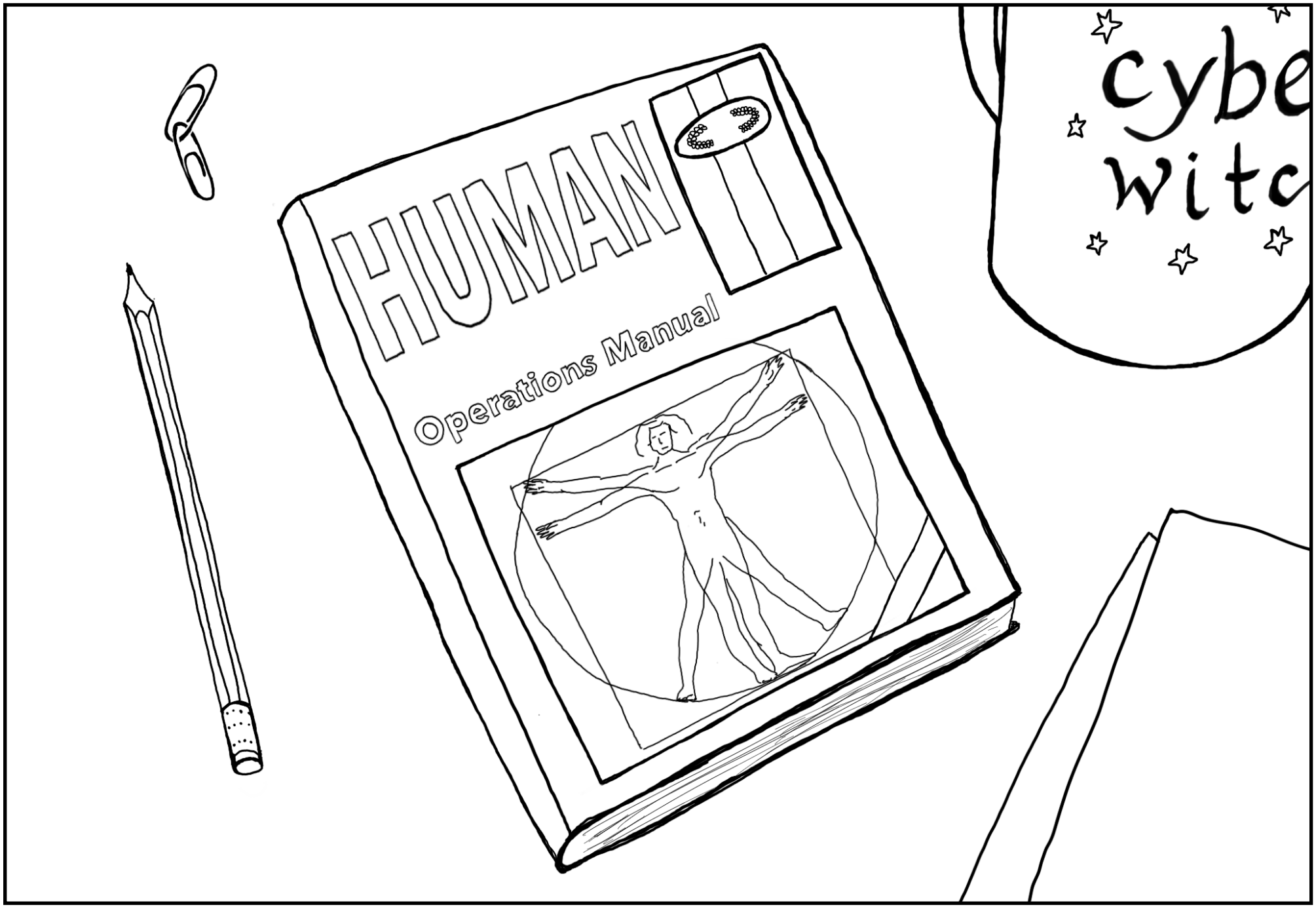
Protecting people is hard. We usually secure things by keeping them under tight control, but people are unpredictable and uncontrollable.

So to make our job easier, we often don't treat people as an integral part of our systems. They're just "users" – an extension of the interface they happen to be using.

And when they make mistakes, we blame them, not ourselves – "They should have been more careful. How can they be so stupid?"

But what if people aren't the problem? What if they're prone to making mistakes because we aren't doing our part to keep them safe, the way we do with the rest of our systems?

To help keep people safe, we need to understand how they work. So let's take some time to learn more about the most important and vulnerable part of our network – people.


HUMAN
Operations Manual
cybe
witc

We tend to think of our brains working like computers.

But human brains don’t work like computers.

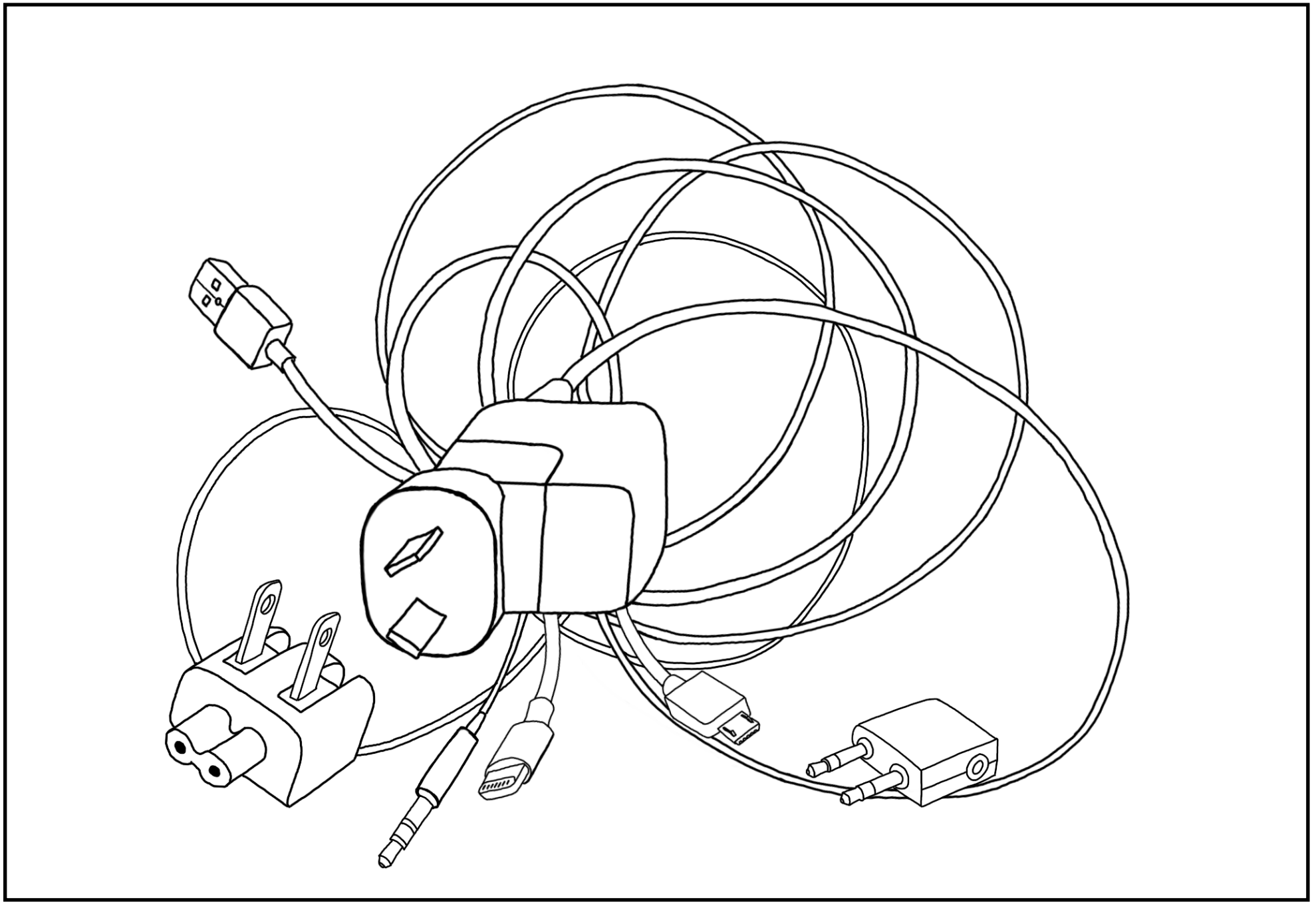
Computer programs process information according to defined rules.

We make sense of the world by making connections to things we already know.

We pick out things that seem relevant, compare it to our past experience, and fill in the gaps through creativity and imagination.

This is how we’re able to respond to situations we’ve never encountered or even imagined before.

Sometimes we make mistakes – and that’s fine. Trying, failing and adapting is how we learn new skills!



Security is all about managing risk, which is something people aren't great at judging.

In new situations our brains are alert to our surroundings, so we can take everything in and work out if it might be important – a threat or an opportunity.

It would be exhausting to do that all the time so when things are routine or familiar we tend to relax, and only notice things that seem especially out of place.

We tend to feel safe when things are familiar, and don't want to overreact if something feels a little out of place – it's probably nothing, right?

People will make mistakes if they have to maintain constant vigilance while doing routine things. We can help by making it easier to speak up and get a second opinion when things don't seem quite right.

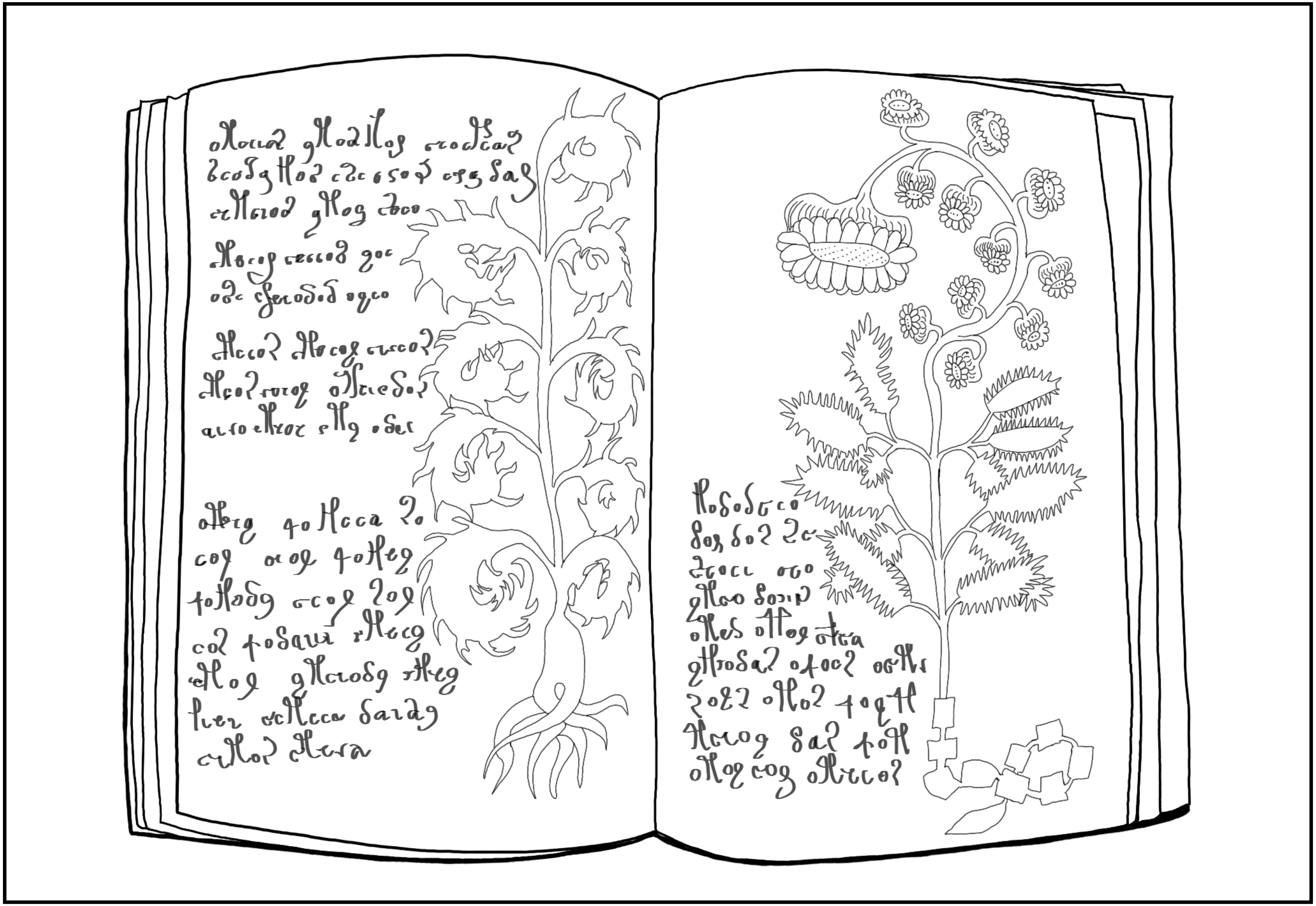

To Troy
from Greece
xoxo

Meet the mysterious Voynich Manuscript. It's a 15th century botanical text written in an unknown script that no-one has ever managed to decipher. It's confounded linguists and code crackers for centuries.

If it is a hoax it's a clever one - when people try to make things up, we tend to do so in ways that are predictable, and the Voynich Manuscript's text has the patterns of a real language, but no-one has been able to identify or decipher it yet.

Computers can identify when people are making things up - like arbitrarily picking test answers or falsifying research data - because our brains tend to use predictable systems to do so.

It's the same with things like passwords. For years people were told to choose complex, random passwords. Many people thought they were doing the right thing to protect their accounts but they used methods that felt random but were easy for computers to guess.



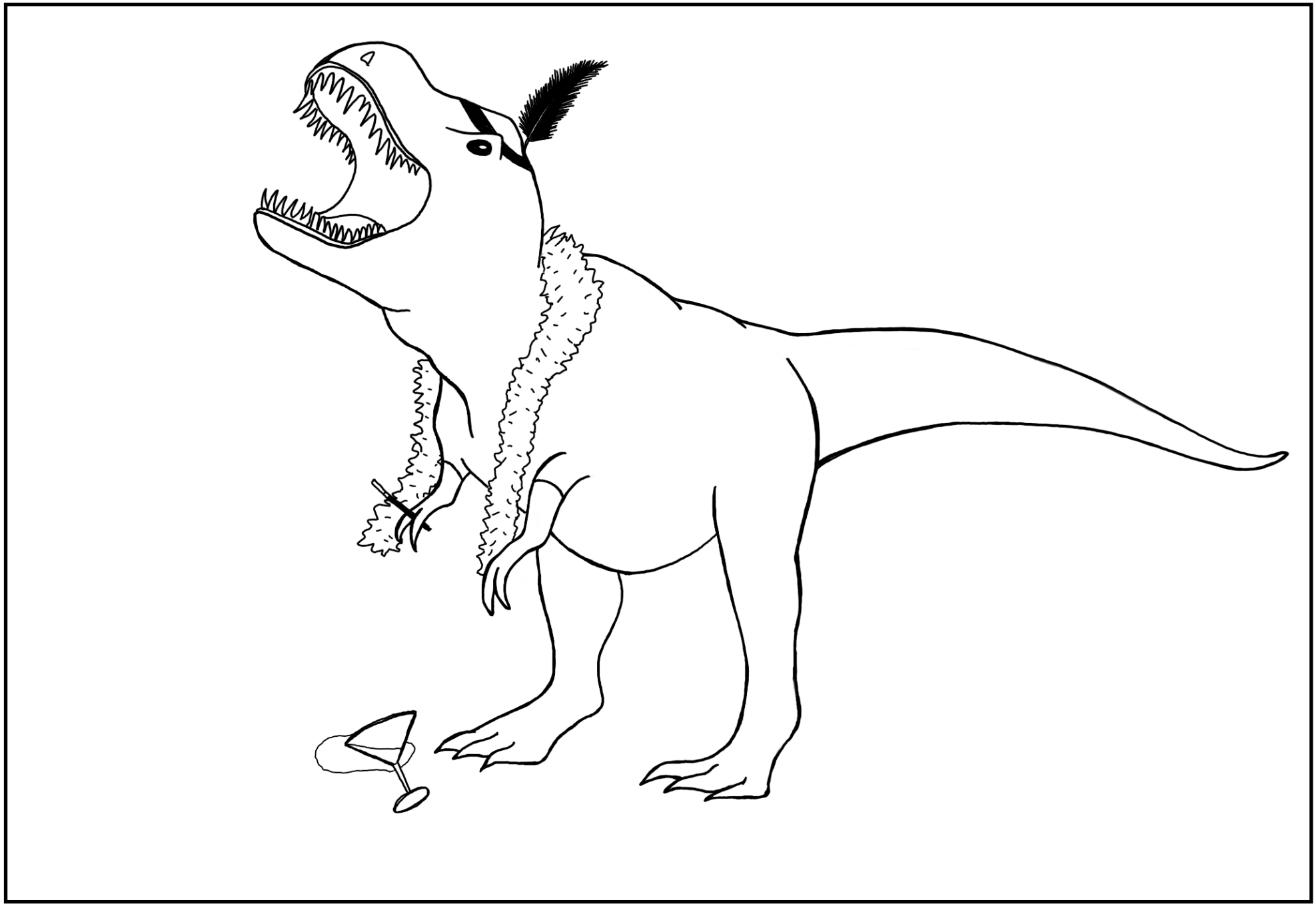
When we know something isn't working, like getting people to choose complex passwords, we change our advice. But it can be hard to get people to unlearn things and change their ways.

This phenomenon is called belief perseverance.

If you imagine a Tyrannosaurus Rex you probably imagine it looking like a lizard, even though you've since learned they had feathers. The first thing you learned sticks in your brain and it takes a lot to shift it. That's belief perseverance in action.

So it isn't enough to tell people they should use passphrases and password managers when they "know" passwords shouldn't have dictionary words or be written down.

It takes time to guide someone through the thought process to understand why the advice has changed. But it's important if you want them to change their behaviour.



We can all learn some things about security culture from the pukeko.

Unlike most ground-based New Zealand birds, the pukeko population is thriving - because pukeko take security seriously.

They form communities and lay their eggs in a communal nest that everyone keeps an eye on. No single points of failure here.

If anyone spots a threat they raise the alarm so the whole community knows and the adults can fight off the threat. Pukeko have been observed protecting their young from falcons, cats and stoats!

Everyone in the pukeko community has a role to play in keeping everyone safe, and everyone knows what they need to do if they spot something that could be a threat.

So how can we make our people more like pukeko?

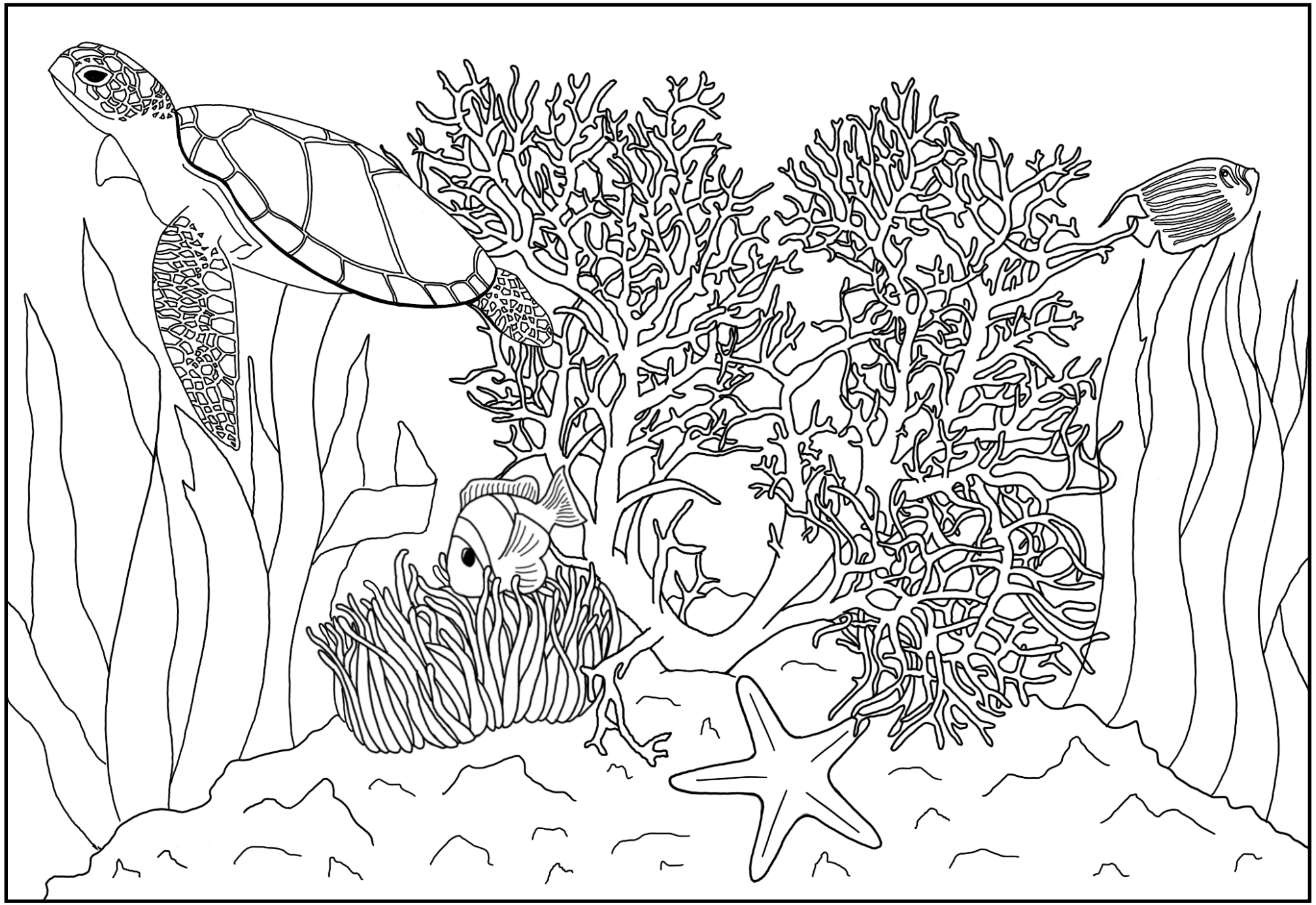

we take security seriously.

There’s so much we need to do to to keep our systems secure, and the threats are unknown and constantly evolving. How do you get people to care about security when it feels so overwhelming?

Do you take your own bags to the supermarket? Small individual actions like reusing bags don’t have a huge impact on their own, but that’s not the point. These small acts give ordinary people a way to be part of the solution to overwhelming problem. And when people feel like they’re doing something and the people with the real power to change things *aren’t*, they start to demand bigger changes, even if those changes might have a cost or inconvenience them.

Remember the ozone hole? It’s finally starting to shrink – but only because people cared enough to demand that industries stop using the gases that were causing the hole to grow.

Is there something you can change to make people feel like they’re part of the solution and start expecting others to do the same?



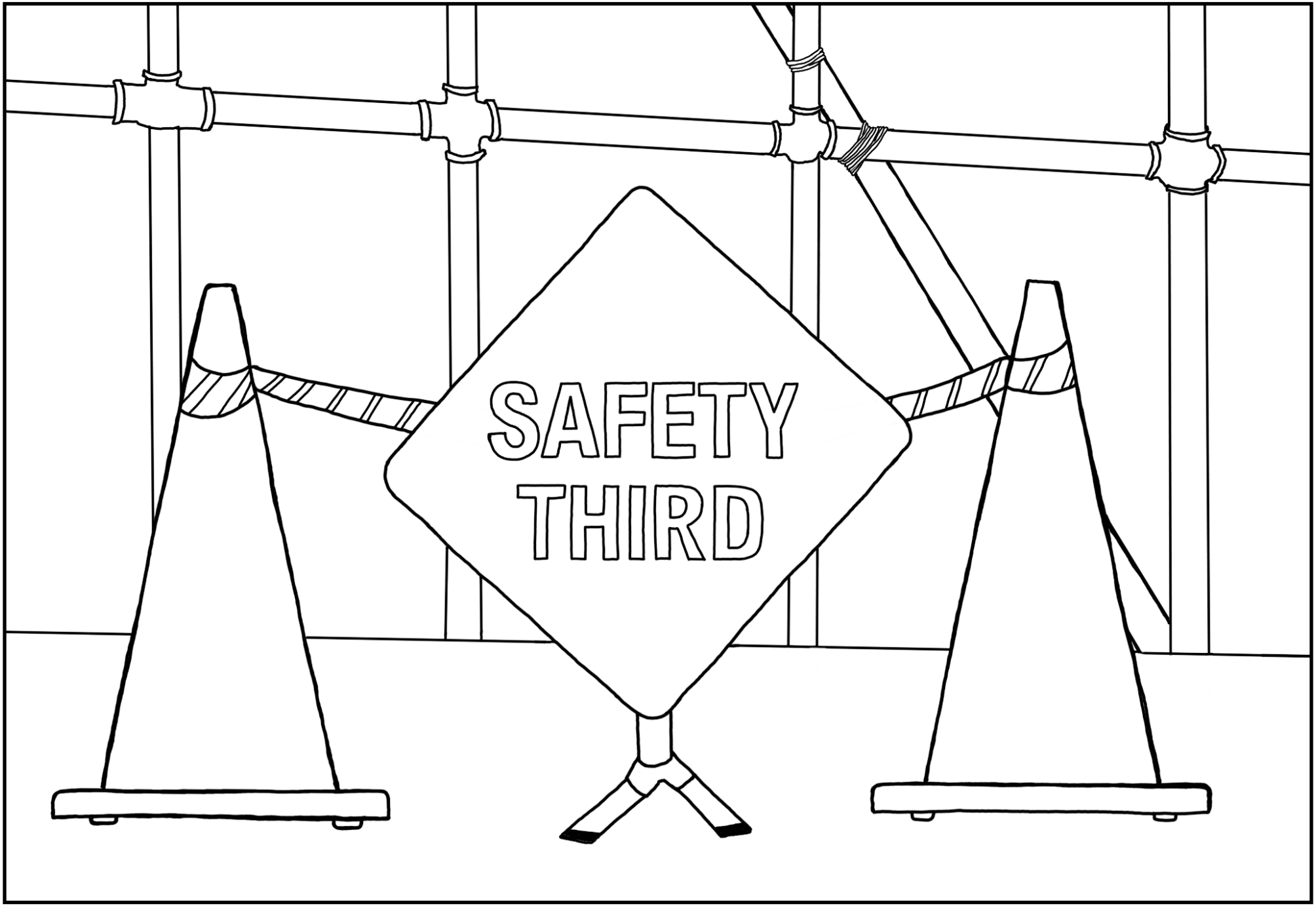
We get more of the behaviours we reward. You can't expect people to put safety first when they have incentives to ignore it.

What does your organisation *really* value? If it "doesn't have time" for security because speed is paramount, start tallying up the time spent on fixing security issues before they become a big problem.

If people are worried about sticking out for going against the office culture, pick out the influencers – they might be bosses, or people others look to as an example – and try to get them onside first.

Safety First might not be achievable, but if you can find ways to work with the organisation's explicit and implicit values, you can create a culture of Safety Third, and still make good things happen.

Don't just imagine why people might not be putting security first. Get out there and ask them. Build relationships and encourage people to let you know when your advice isn't working for them.

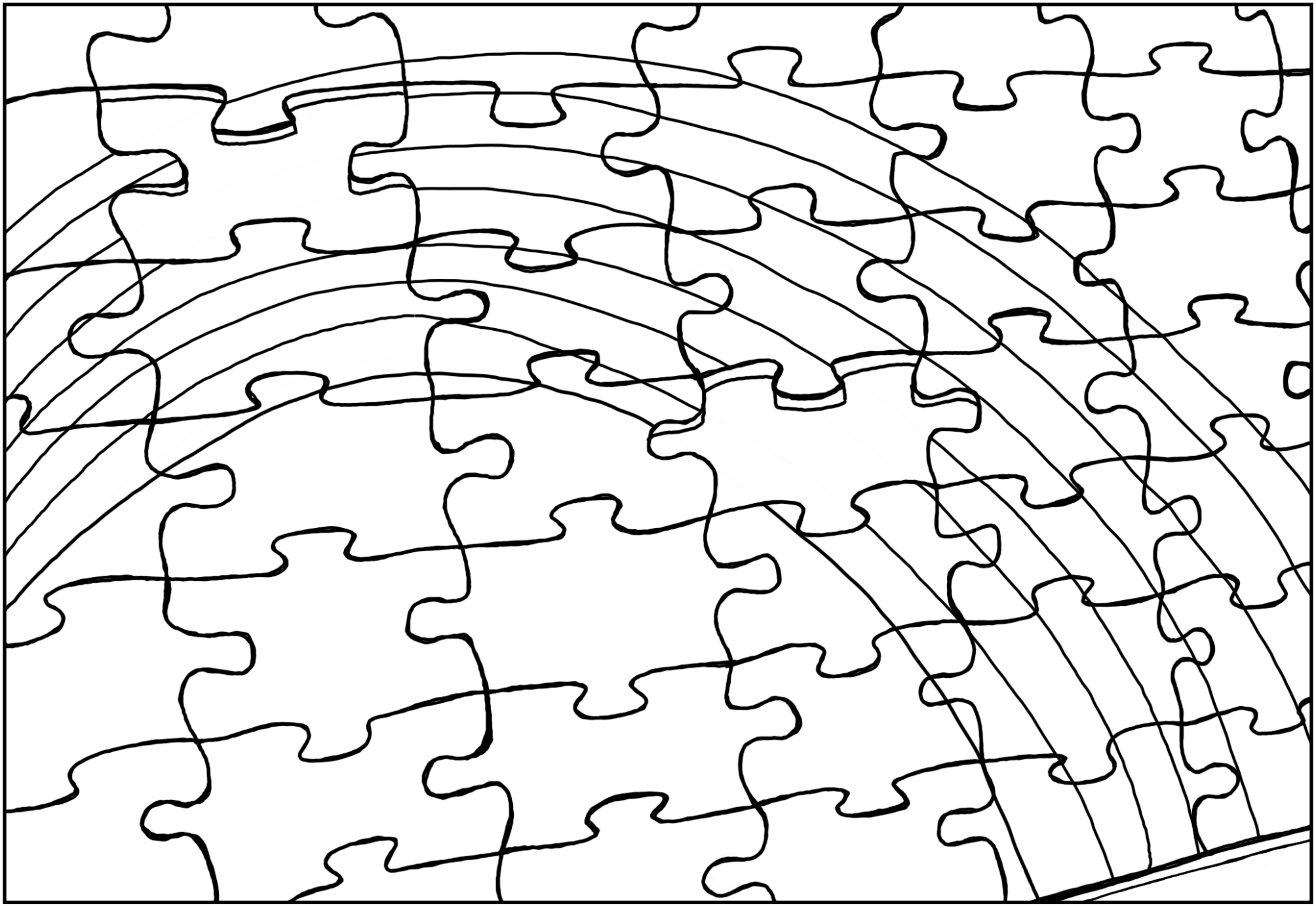

SAFETY
THIRD

People are only human.

We’re vulnerable to making mistakes because our brains don’t process information in an orderly way like a computer, but by making connections to what we already know and taking shortcuts to save effort.

We’re reward-motivated, and that makes it very hard to get people to do things they *should* be doing if there are incentives to not do the right thing.

Instead of trying to make people act more like computers, we need to embrace their humanness. Make connections with people. Equip them with the tools they need to make a difference, listen to them to understand why things aren’t working, and build systems and a culture that tolerate mistakes so people can fail and learn without fear of being blamed and shamed.



Advanced Endpoint Protection: Securing The Meaty Bits was written and drawn by Petra Smith.

This colouring book was created to accompany a presentation first given at Purplecon, an actionable defensive information security conference held 15 November 2018 in Wellington, New Zealand.

Thanks to the Purplecon crew and volunteers, Kirk for proofreading and prooflistening, and all the folks at Aura Information Security.