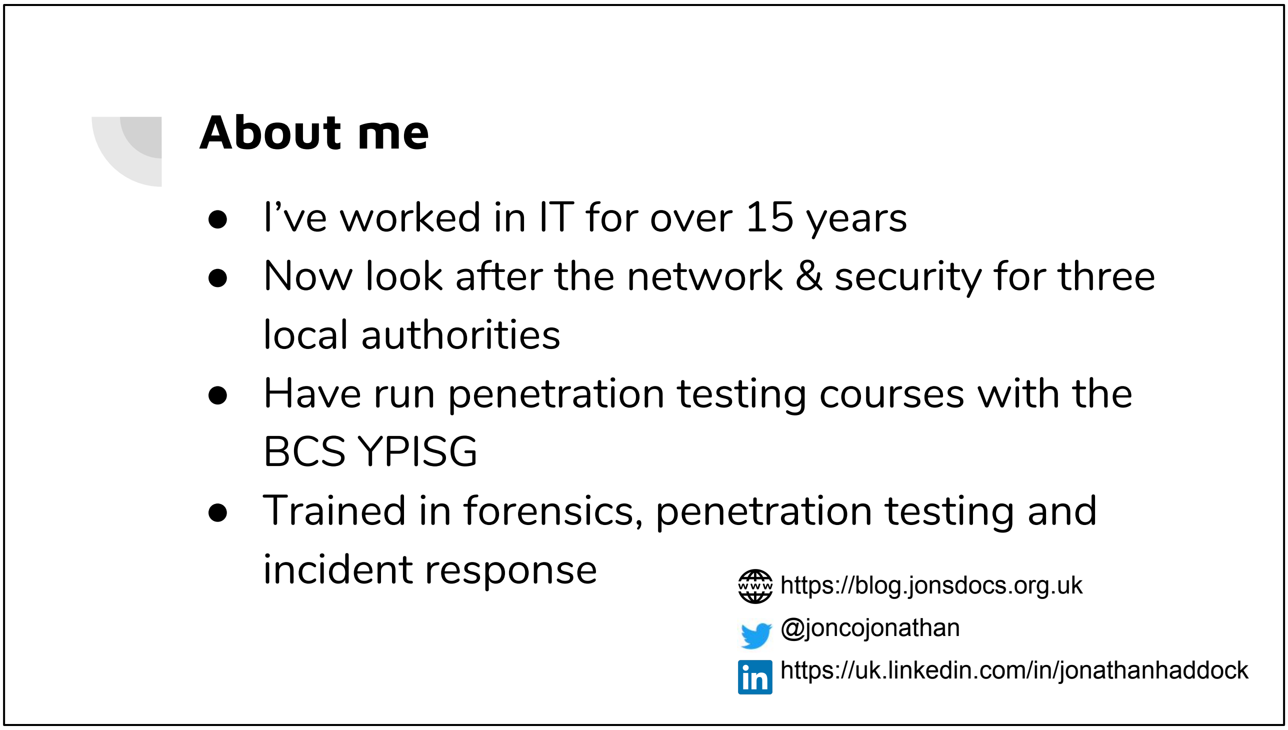
The Threat of Security Knowledge Gaps

Jonathan Haddock
11th January 2019

In this presentation I'll look at what a security knowledge gap is, some of the places they exist and suggest possible solutions to them. This is based on my experience and isn't a definitive or exhaustive list. There's also areas for me to work on too, so please don't think I'm presenting myself as perfect - I'm speaking to myself too!

While not knowing something isn't in itself a new problem, I'd suggest it was an emerging problem for cybersecurity as attention paid to security problems increases.



About me

- I've worked in IT for over 15 years
- Now look after the network & security for three local authorities
- Have run penetration testing courses with the BCS YPISG
- Trained in forensics, penetration testing and incident response

https://blog.jonsdocs.org.uk

@joncojonathan

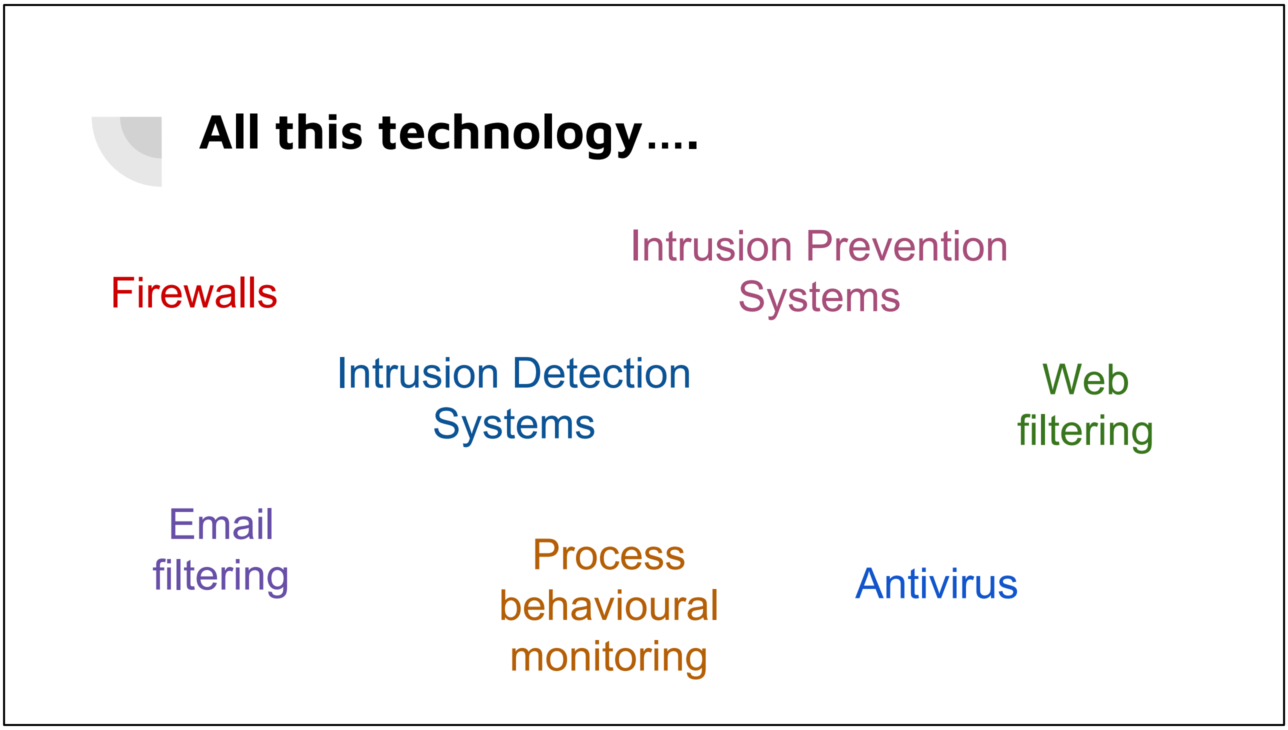
https://uk.linkedin.com/in/jonathanhaddock

The YPISG is a BCS specialist group - Young Professionals' Information Security Group.

Every role helps with security, whether that's on the service desk or as a developer. I've worked across a number of roles, starting in service desk / desktop support, and each has benefited from experience gained in the others.

If you want to get into IT security, I recommend you specialise in an area you find interesting but make sure you keep your hand in other areas too so you have a broad skill set and knowledge. This will allow you to have informed discussions with different teams, in a way they (and you) can understand.

I also blog about cyber security, development, IT, and occasionally local history at https://blog.jonsdocs.org.uk.



All this technology....

Firewalls

Intrusion Prevention Systems

Intrusion Detection Systems

Web filtering

Email filtering

Process behavioural monitoring

Antivirus

Despite all the security technology we have installed in our organisations there are still problems. New breaches are announced almost weekly but often you can't blame the security tools installed on the network - humans play a significant factor.

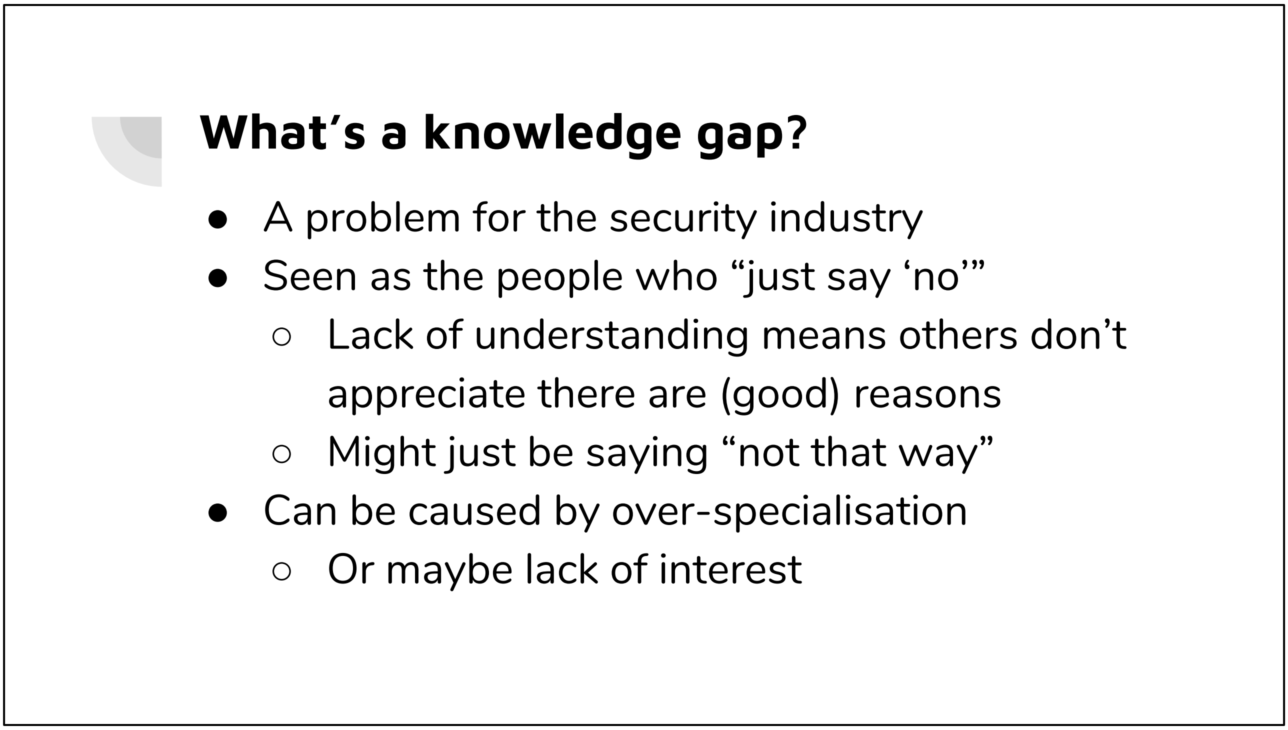
At the end of the day, people have to build the environment and that's when mistakes can be made. By increasing awareness of security across the board it's possible to reduce these mistakes, possibly offsetting some.

Where this presentation refers to "security", it should be noticed I'm referring specifically to cybersecurity / information security, and not anything else.

What’s a knowledge gap?

- Where one group knows something the other doesn’t
  - Lack of “information parity”
- Works both ways round
  - Security → Other teams
  - Other teams → Security

It’s really important to note gaps work in both directions. Other teams may not implement things the way a security team would like as they don’t know any differently. Equally, the security team might be unknowingly making demands another team simply can’t make (limitations in technology, budget or time).



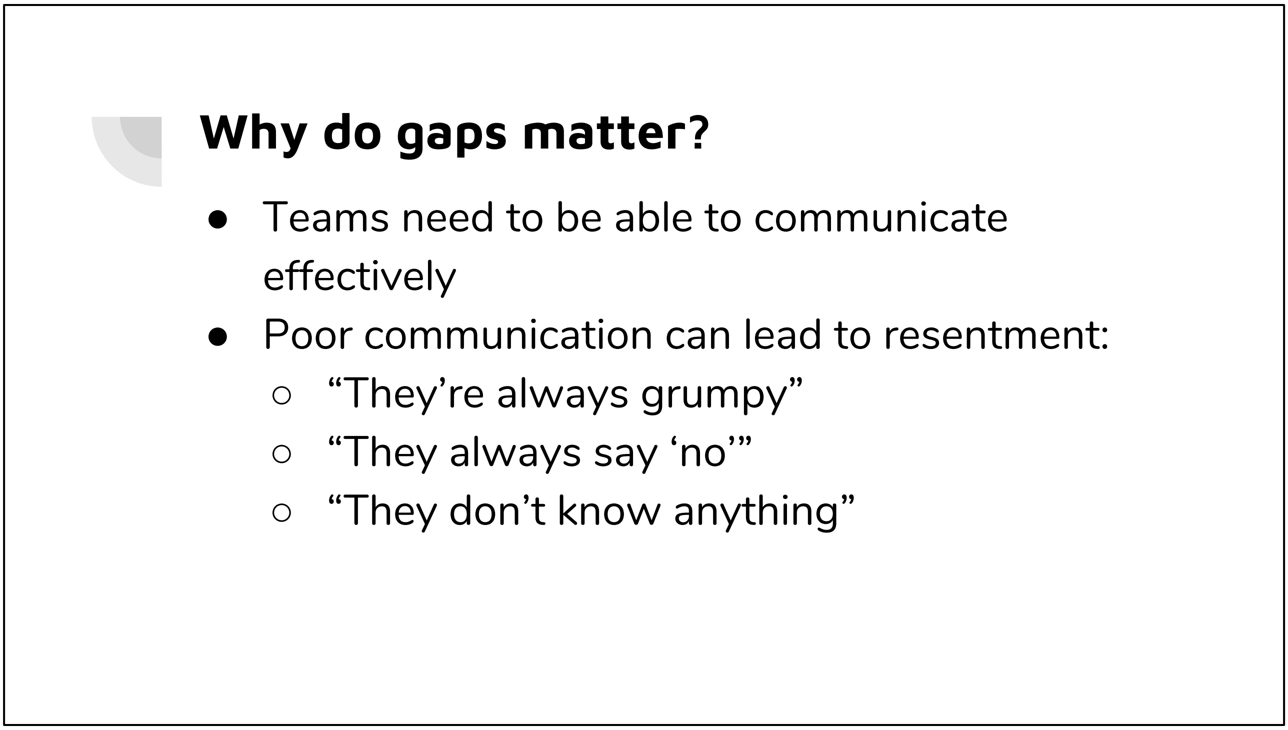
What’s a knowledge gap?

- A problem for the security industry
- Seen as the people who “just say ‘no’”
  - Lack of understanding means others don’t appreciate there are (good) reasons
  - Might just be saying “not that way”
- Can be caused by over-specialisation
  - Or maybe lack of interest

Security teams have a bad reputation as people that just say no or prevent users from working, but what’s important to note is that’s very rarely what’s going on. Often it’s a case of “that way’s not secure, do it this way”. Security engineers that always say “no” only achieve creativity on the part of their users, finding a way around the block.

Over specialisation is a blessing and a curse. Knowing your subject matter really well is always good, but having only a tiny amount of knowledge of other areas hampers collaborative working.

Lack interest can be a personal choice. The challenge for organisations is how to get their staff to want to learn and feel engaged.



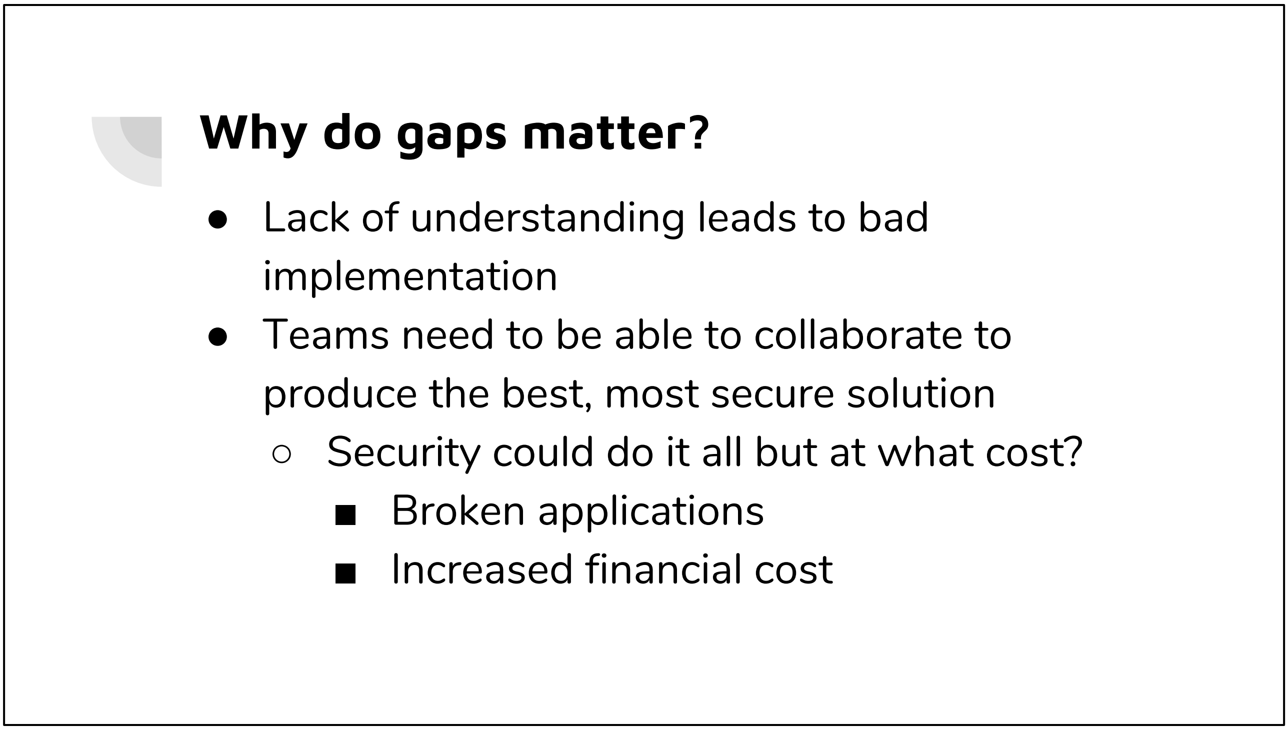
Why do gaps matter?

- Teams need to be able to communicate effectively
- Poor communication can lead to resentment:
  - “They’re always grumpy”
  - “They always say ‘no’”
  - “They don’t know anything”

The IT industry has plenty of jargon to start with, but then cybersecurity adds a whole lot more. Encryption, private keys, certificates, PGP, signature - list list goes on. To communicate effectively we need to reduce our use of jargon, or make sure it’s well explained.

If teams resent each other, or just simply dislike the interaction, systems won’t be implemented in the best possible way (be that securely or to best effect). I’ve worked in environments where the security team is considered an unnecessary blocker to getting things done.

Ultimately we all have to get on and work together. Having a bit of understanding of each discipline can really help facilitate that.

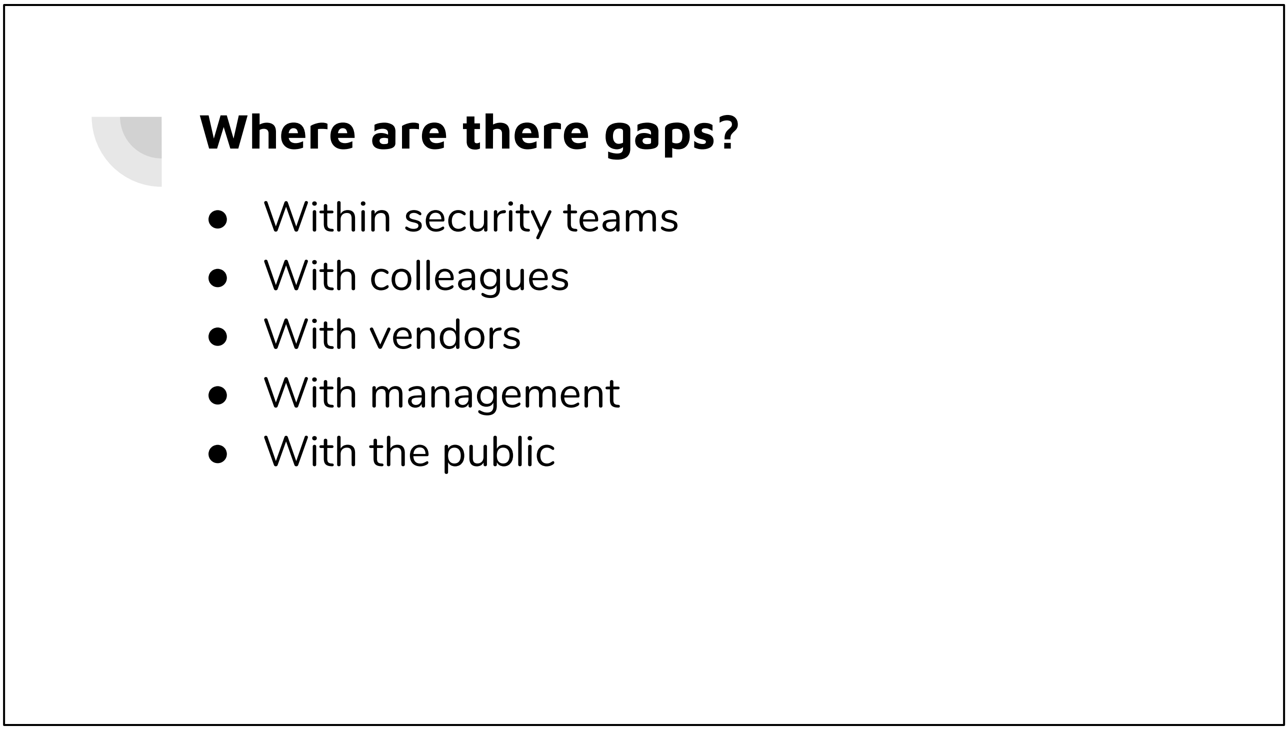


Why do gaps matter?

- Lack of understanding leads to bad implementation
- Teams need to be able to collaborate to produce the best, most secure solution
  - Security could do it all but at what cost?
    - Broken applications
    - Increased financial cost

When another team doesn't understand what your security requirements mean they might try their best guess. This can lead to an "oh, like that?!" moment as they realise they didn't (and you realise the security team failed at communicating, possibly).

The security team could just implement every system - at least it would be secure. The downside is that they probably don't know the application very well, so it's unlikely to work. Cybersecurity staff are often paid more too, so the increased financial cost, combined with a non-working system, would be an immediate problem to the business.



Where are there gaps?

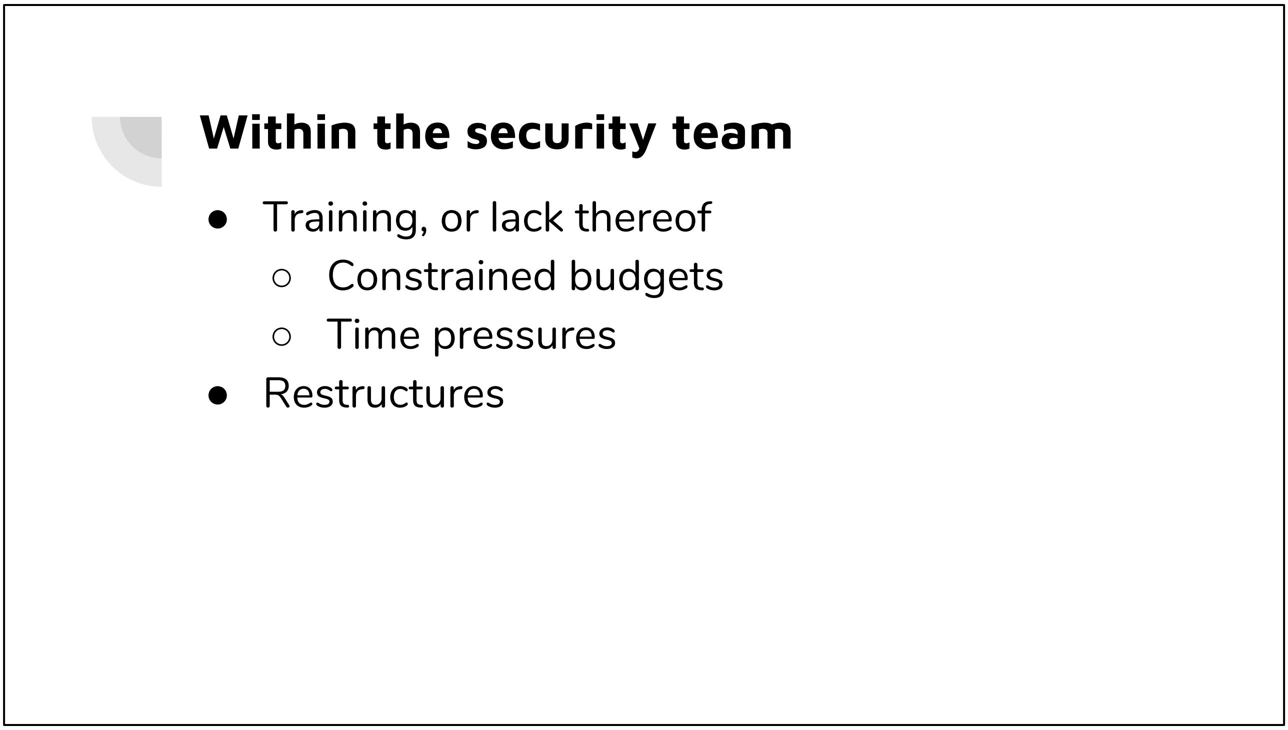
- Within security teams
- With colleagues
- With vendors
- With management
- With the public

Gaps happen everywhere, this is just a few examples.

Causes of the gaps can overlap, so where some are identified here that's not to say the cause only applies to that interaction. Similarly, some of the solutions probably work across the board.

Another gap that exists, not covered so obviously, is between the security team and would be attackers - potentially a talk in itself.

Gaps for the security team

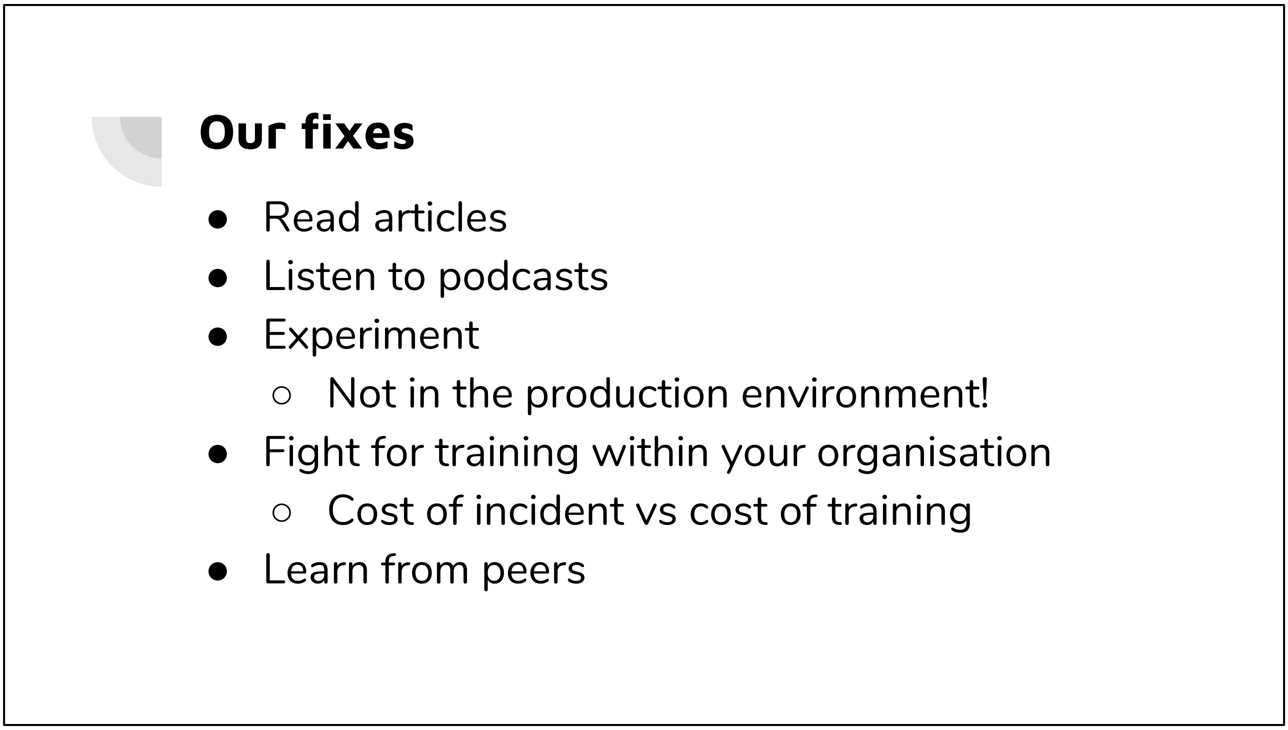


Within the security team

- Training, or lack thereof
  - Constrained budgets
  - Time pressures
- Restructures

It makes sense to start by looking at the security team itself. In current climate, particularly in the public sector, budgets are being squeezed. As a result, staff numbers are going down, workloads are going up and budgets decrease. In my case, the entire IT training budget for the year is £10,000 which, given training vendors often charge £2,000 (ex VAT) per person for a week-long course means that's not a lot of training. With workloads going up it's harder to fit the training in too.

Some staff may have been put in their current position following a restructure - the post holder may have no cybersecurity training or experience whatsoever.



Our fixes

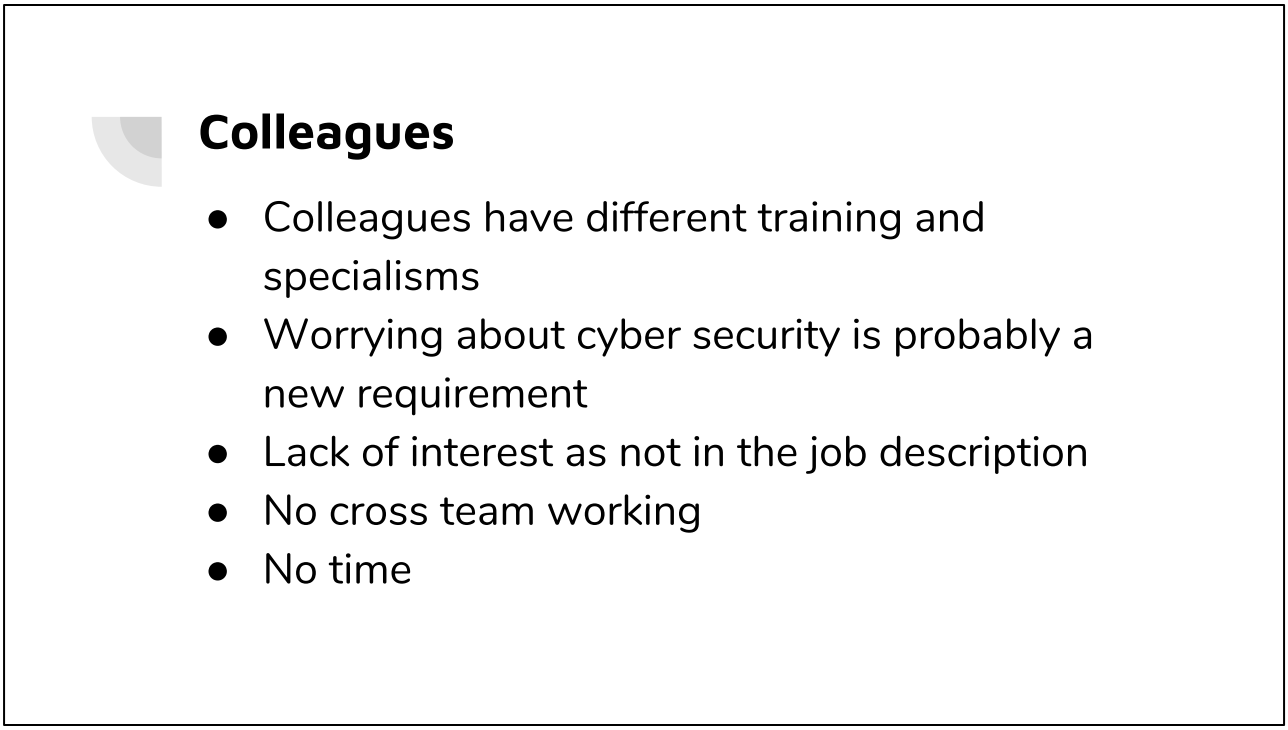
- Read articles
- Listen to podcasts
- Experiment
    - Not in the production environment!
- Fight for training within your organisation
    - Cost of incident vs cost of training
- Learn from peers

There’s a lot of free material out there, and I recommend blogs from people like Troy Hunt and Scott Helme (to name just two). There’s absolutely nothing wrong with using blogs as useful references and it’s how our industry seems to be presenting a lot of information at the moment. Spend some time finding security minded people and have a flick through their posts; they often come up when searching for the problem you’re facing anyway.

If you have a commute, or an office where it’s agreeable to listen to podcasts, then that can also be a good way to keep track of security news. A podcast may take longer to publish than a blog post, but it’s still useful. Links to two of my recommended podcasts are at the end.

There’s also free courses out there (Troy Hunt has some free ones on Pluralsight, or the Metasploit Unleashed course (donation suggested). If a free course doesn’t cut it, fight for training. You want your employer to be investing in your development - it benefits both of you. Peer learning is really powerful too, so don’t be afraid to learn from colleagues.

Gaps with colleagues

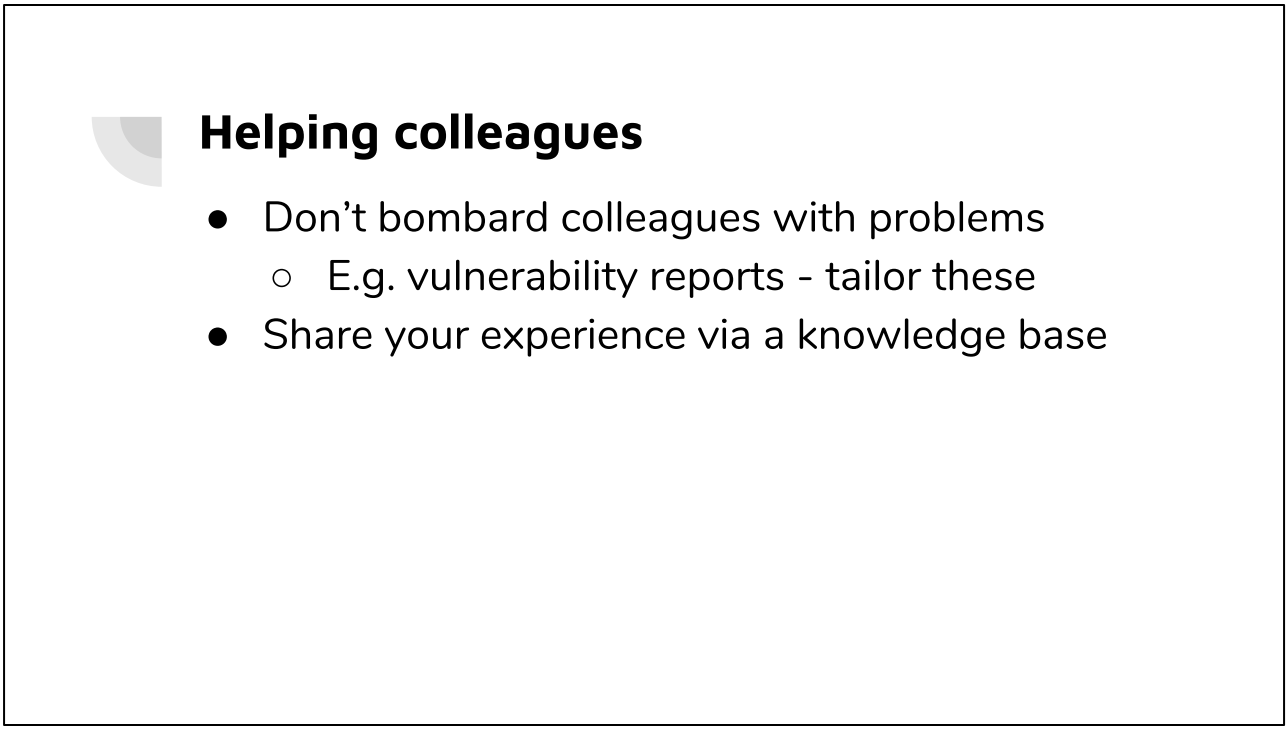


Colleagues

- Colleagues have different training and specialisms
- Worrying about cyber security is probably a new requirement
- Lack of interest as not in the job description
- No cross team working
- No time

Consider that your colleagues have different priorities, as well as different training. The security team is about to give them a lot more work, and it’s probably work they’ve never done before.

I hear a lot of “that’s not in my job description” but can see the time that IT departments write in clauses like “implement secure systems, taking advice from the security team” not being that far off. That said, we can’t shout at someone if they play the “not my job” card, we need to work with them.



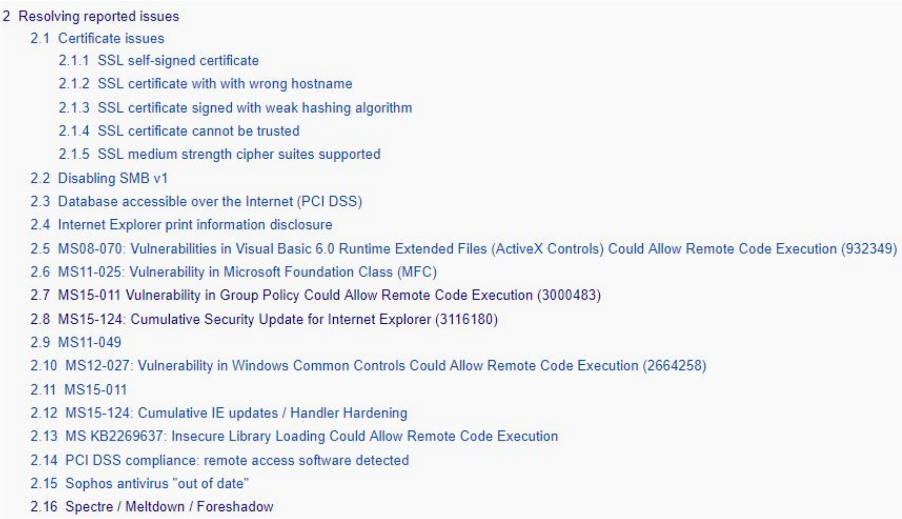
Helping colleagues

- Don’t bombard colleagues with problems
  - E.g. vulnerability reports - tailor these
- Share your experience via a knowledge base

If we bombard our colleagues with new information or problems, say the results of a vulnerability scan, we will just overwhelm them. Tailor what problems you pass to your colleagues, and offer advice wherever you can. The list of problems will go down, so chip away at it rather than trying to do it all at once.

Given the security team probably knows some of the fixes, share them.

Helping colleagues

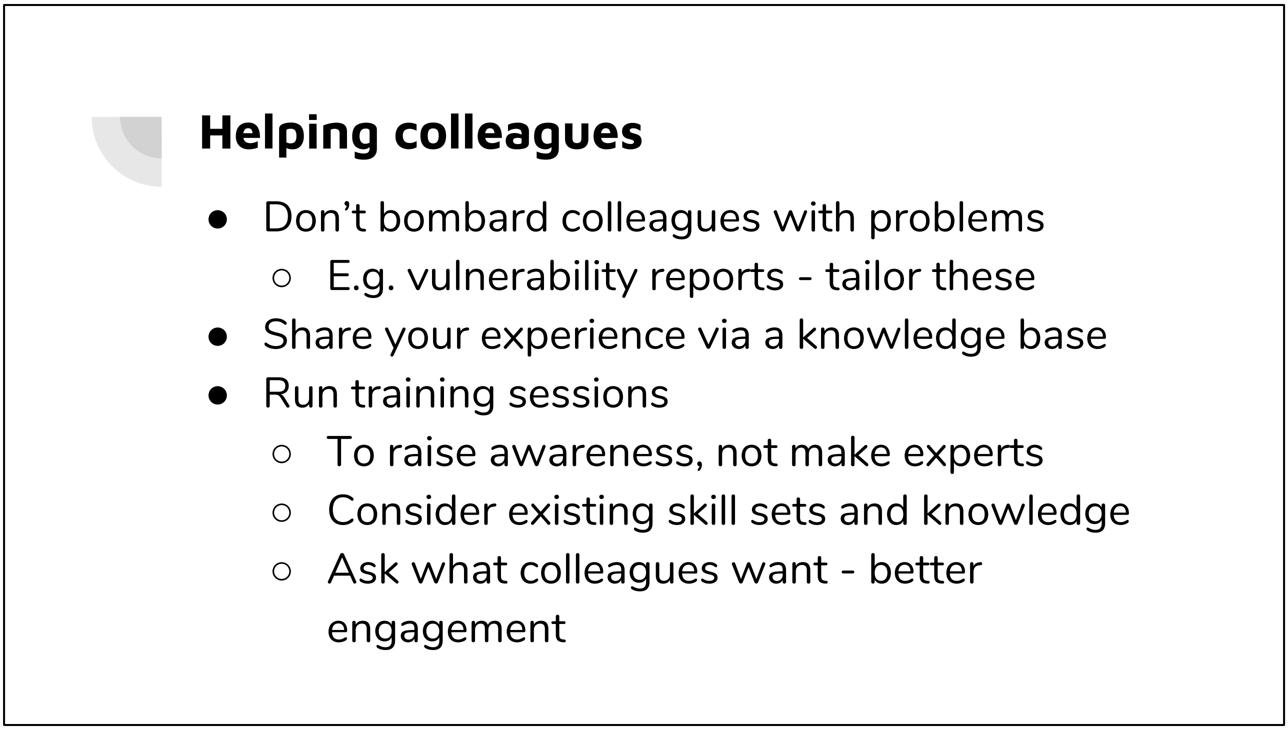


2 Resolving reported issues
- 2.1 Certificate issues
  - 2.1.1 SSL self-signed certificate
  - 2.1.2 SSL certificate with with wrong hostname
  - 2.1.3 SSL certificate signed with weak hashing algorithm
  - 2.1.4 SSL certificate cannot be trusted
  - 2.1.5 SSL medium strength cipher suites supported
- 2.2 Disabling SMB v1
- 2.3 Database accessible over the Internet (PCI DSS)
- 2.4 Internet Explorer print information disclosure
- 2.5 MS08-070: Vulnerabilities in Visual Basic 6.0 Runtime Extended Files (ActiveX Controls) Could Allow Remote Code Execution (932349)
- 2.6 MS11-025: Vulnerability in Microsoft Foundation Class (MFC)
- 2.7 MS15-011 Vulnerability in Group Policy Could Allow Remote Code Execution (3000483)
- 2.8 MS15-124: Cumulative Security Update for Internet Explorer (3116180)
- 2.9 MS11-049
- 2.10 MS12-027: Vulnerability in Windows Common Controls Could Allow Remote Code Execution (2664258)
- 2.11 MS15-011
- 2.12 MS15-124: Cumulative IE updates / Handler Hardening
- 2.13 MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
- 2.14 PCI DSS compliance: remote access software detected
- 2.15 Sophos antivirus "out of date"
- 2.16 Spectre / Meltdown / Foreshadow

Our knowledge base contains details of problems we know get detected by vulnerability scans, and we make details of the fixes available to everyone in IT. There’s no reason for another team to reinvent the wheel.

Some of these sections contain scripts to run, others offer advice and steps to take to mitigate the vulnerability by hand.

Sadly this screenshot was missing from my presentation at the conference.



Helping colleagues

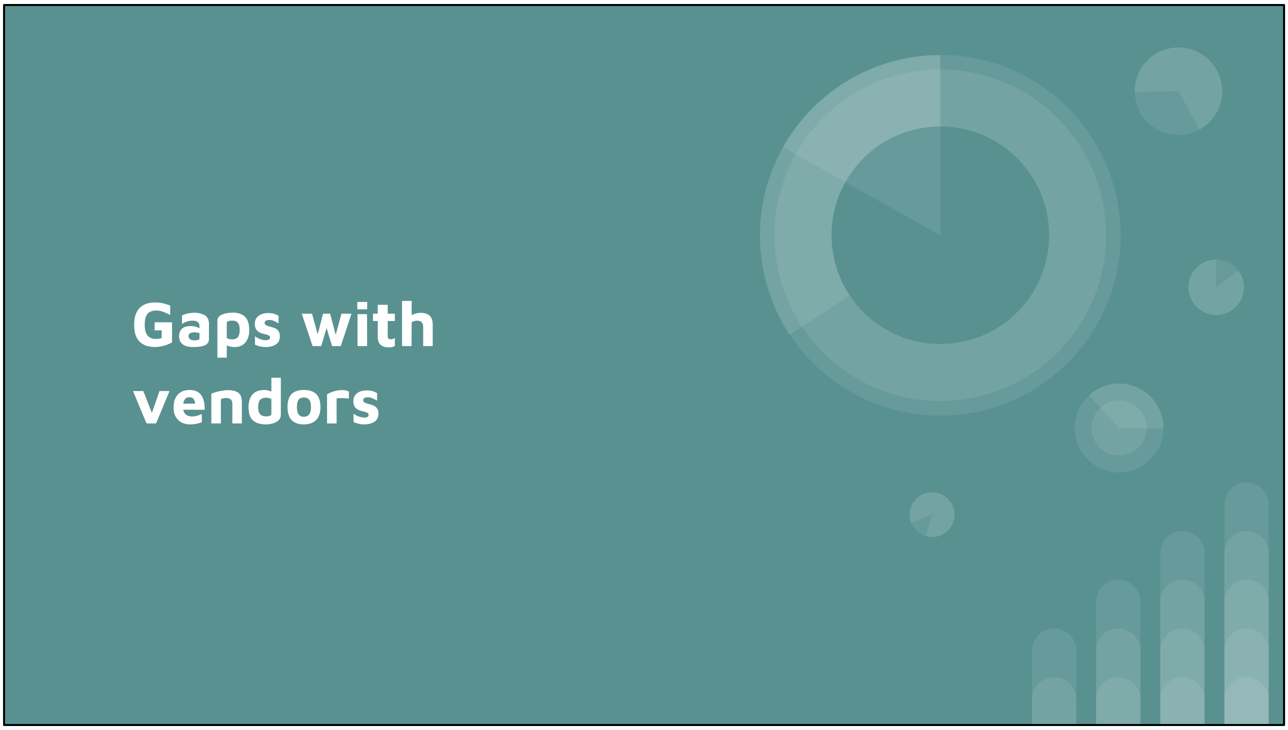
- Don’t bombard colleagues with problems
  - E.g. vulnerability reports - tailor these
- Share your experience via a knowledge base
- Run training sessions
  - To raise awareness, not make experts
  - Consider existing skill sets and knowledge
  - Ask what colleagues want - better engagement

Running training sessions is a great way to share knowledge, either 1 to 1 or in groups. Find out what colleagues are interested in (or what’s causing them the most pain) and target those areas first.

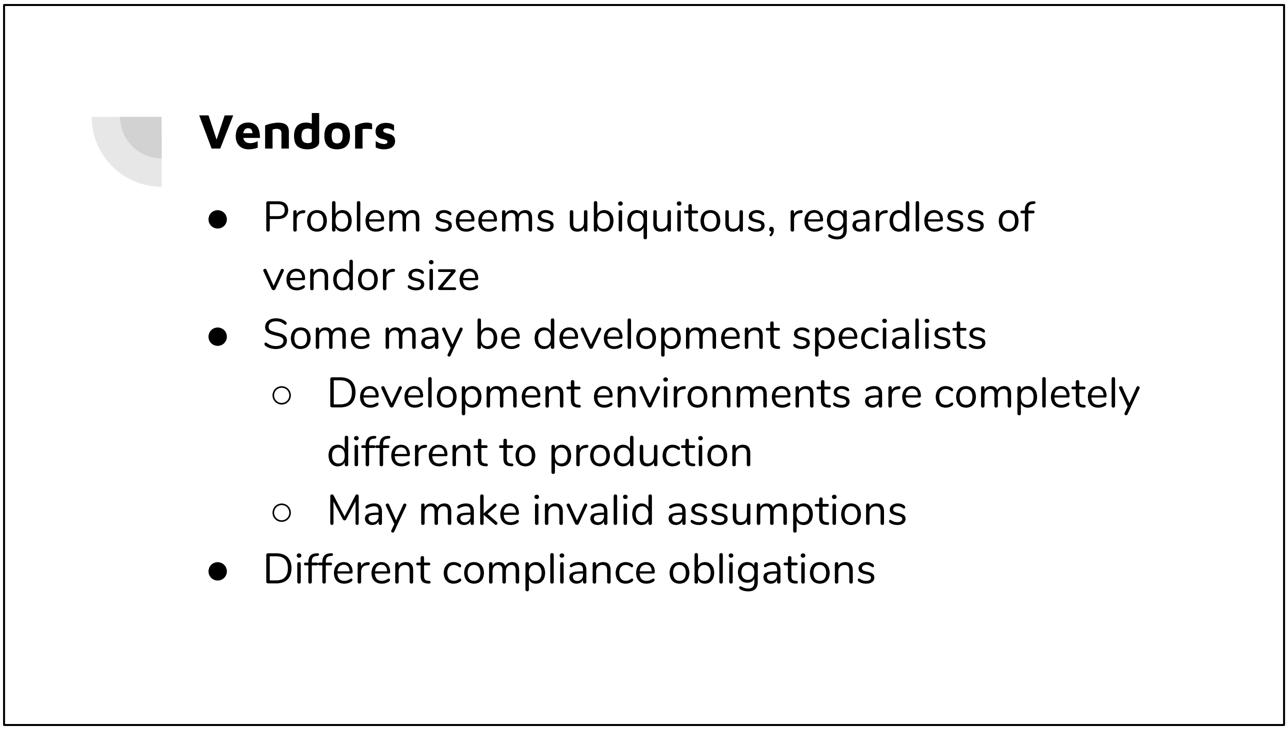
Remember the different skill sets and experiences in your environment and pitch your session accordingly.

Above all

- Get your colleagues on board
- Support them as they embrace new tasks
- Be approachable - there'll be questions
- Reciprocate - they may need help with areas that you just happen to know about



Gaps with vendors

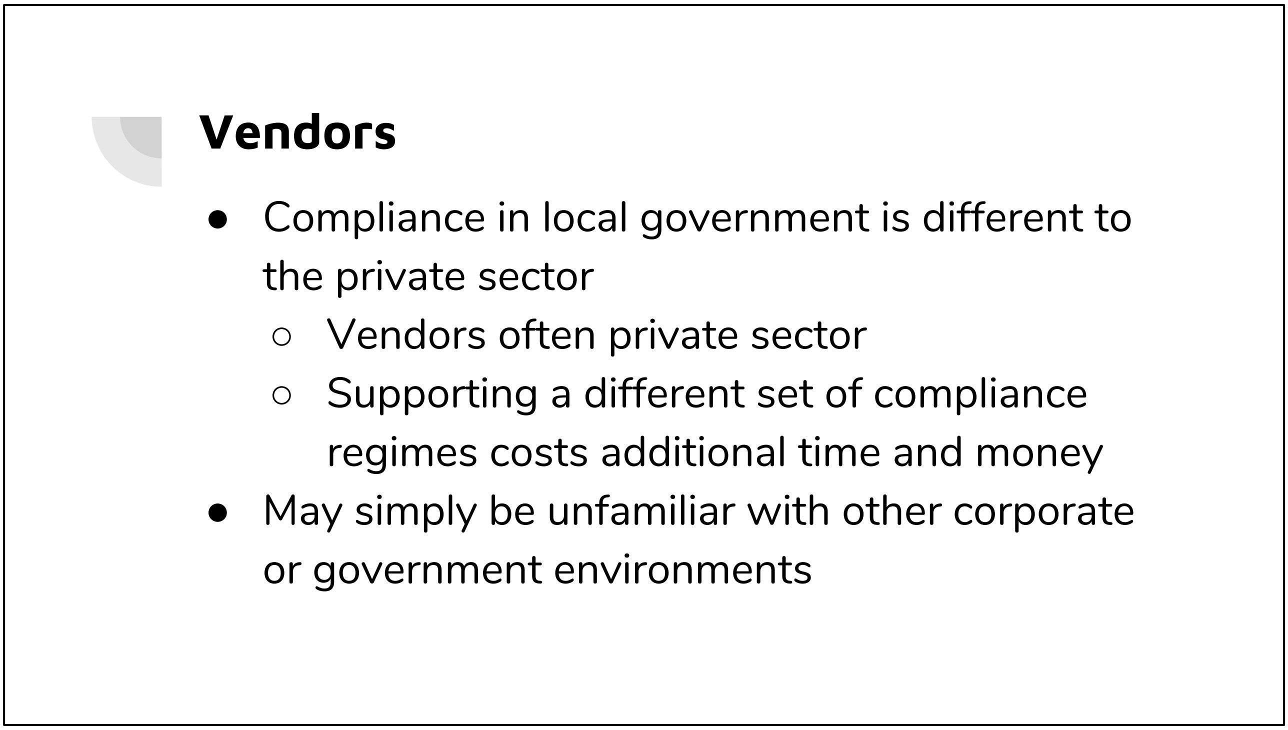


Vendors

- Problem seems ubiquitous, regardless of vendor size
- Some may be development specialists
  - Development environments are completely different to production
  - May make invalid assumptions
- Different compliance obligations

The hardest gap to fix. Vendors are interested in profit and are unlikely to want to pander to each organisation's needs.

Assumptions get made. Some assume all users have admin rights (maybe true 10 years ago, less so now), others assume all connections to the Internet will be permitted, on any port. Often these assumptions are invalid, which trips vendors up.

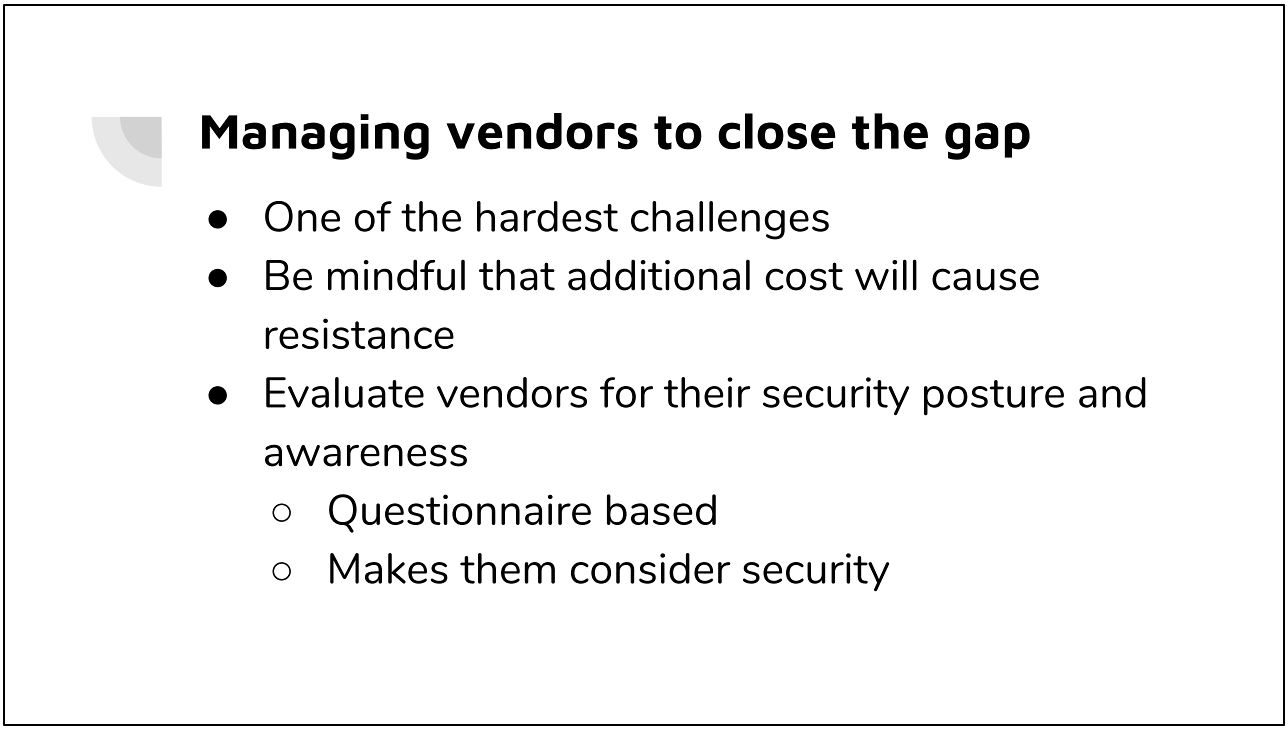


Vendors

- Compliance in local government is different to the private sector
    - Vendors often private sector
    - Supporting a different set of compliance regimes costs additional time and money
- May simply be unfamiliar with other corporate or government environments

Your organisations may have to work in a different compliance space to the vendor. For example, in local government we have to comply with the Public Sector Network code of connection - failure to do so would cut the local authority off from central government resources (benefits systems, DVLA lookups, etc.) meaning everything has to be done by phone and take longer. PCI DSS may apply too, something the vendor (or their developers) may not be used to. These are just some examples, but vendors need to realise compliance can win business.

Sometimes the vendor has a monopoly on a particular application type, so feels they don't need to worry as they'll get the business anyway. That belief needs challenging, for the benefit of everyone.



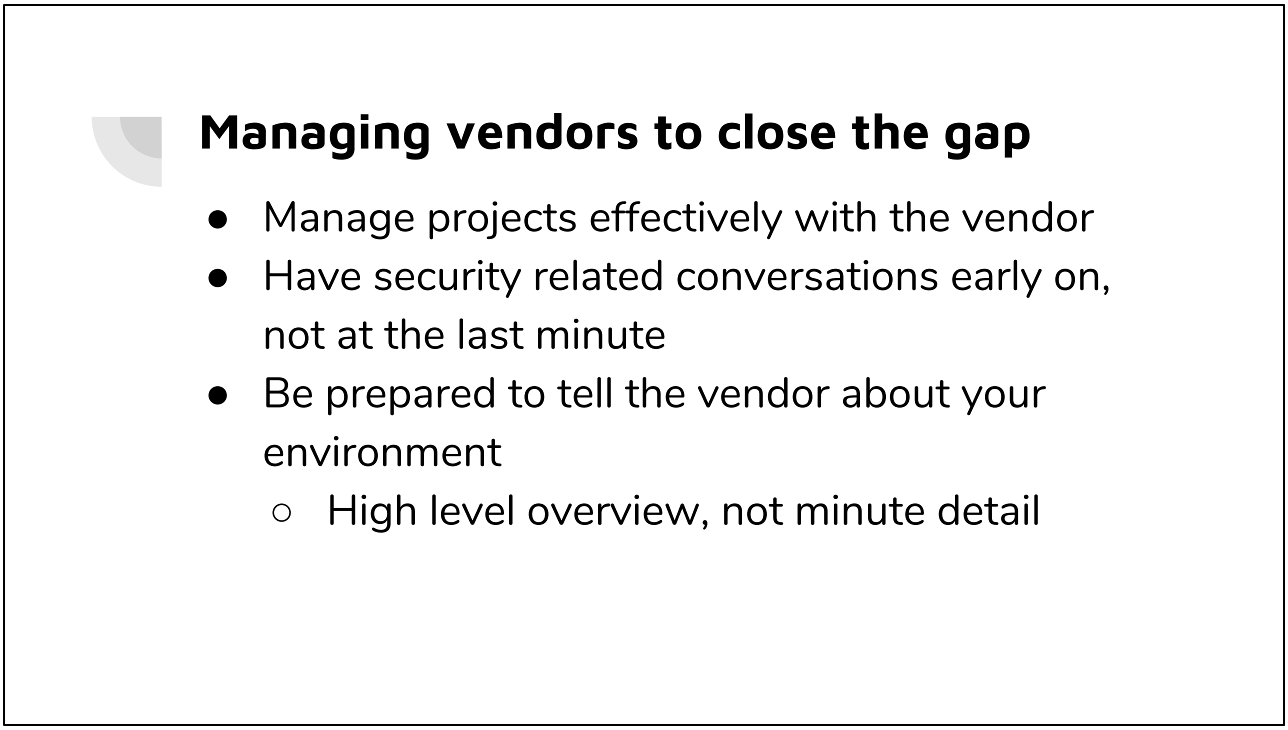
Managing vendors to close the gap

- One of the hardest challenges
- Be mindful that additional cost will cause resistance
- Evaluate vendors for their security posture and awareness
  - Questionnaire based
  - Makes them consider security

In my organisation we provide vendors a questionnaire to complete which asks pertinent security questions. "If a vulnerability is found, how long is it before you issue a patch? What is the cost of that patch?" and questions about the implementation of the system feature on the questionnaire and can highlight areas the vendor hasn't thought of.

Make it easy for the vendor to give that information, but be prepared to challenge any poor answers. We've had to ask why vendors think it's appropriate to not encrypt web traffic before, for example.

During the conference I was asked how we check vendors follow secure development practices. It's a question we've asked vendors before and, in the responses I've seen, is often an area vendors fail at. We've asked if systems have been penetration tested before (and to see the results) and companies can be cagey about sharing that information. The sad fact is, solutions often get purchased even in the absence of these things, as otherwise no solution would be bought. Vendors have a long way to go.



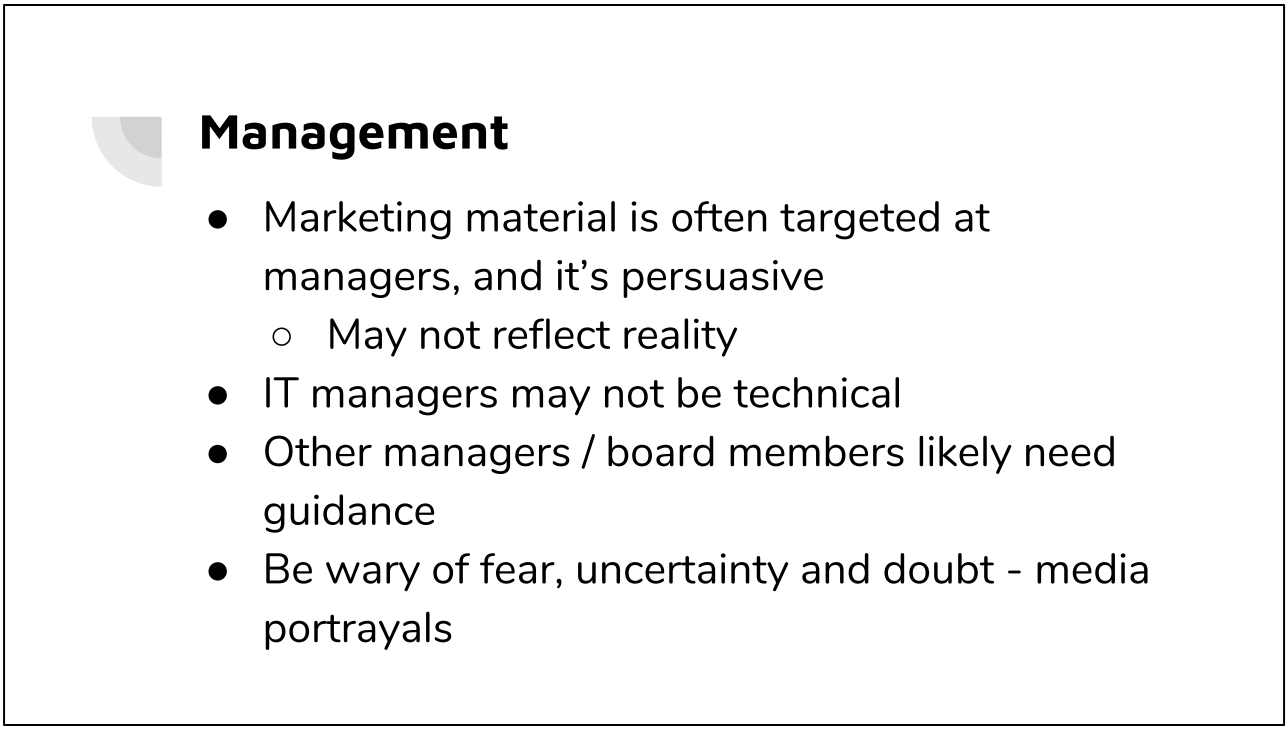
Managing vendors to close the gap

- Manage projects effectively with the vendor
- Have security related conversations early on, not at the last minute
- Be prepared to tell the vendor about your environment
  - High level overview, not minute detail

It’s important to share some information with the vendor so they can better understand your environment. I’m not talking about the absolute, fine details of your environment but an overview. Diagrams can often be a big help.

I’ve blogged about this as a plea to vendors.

Gaps with management



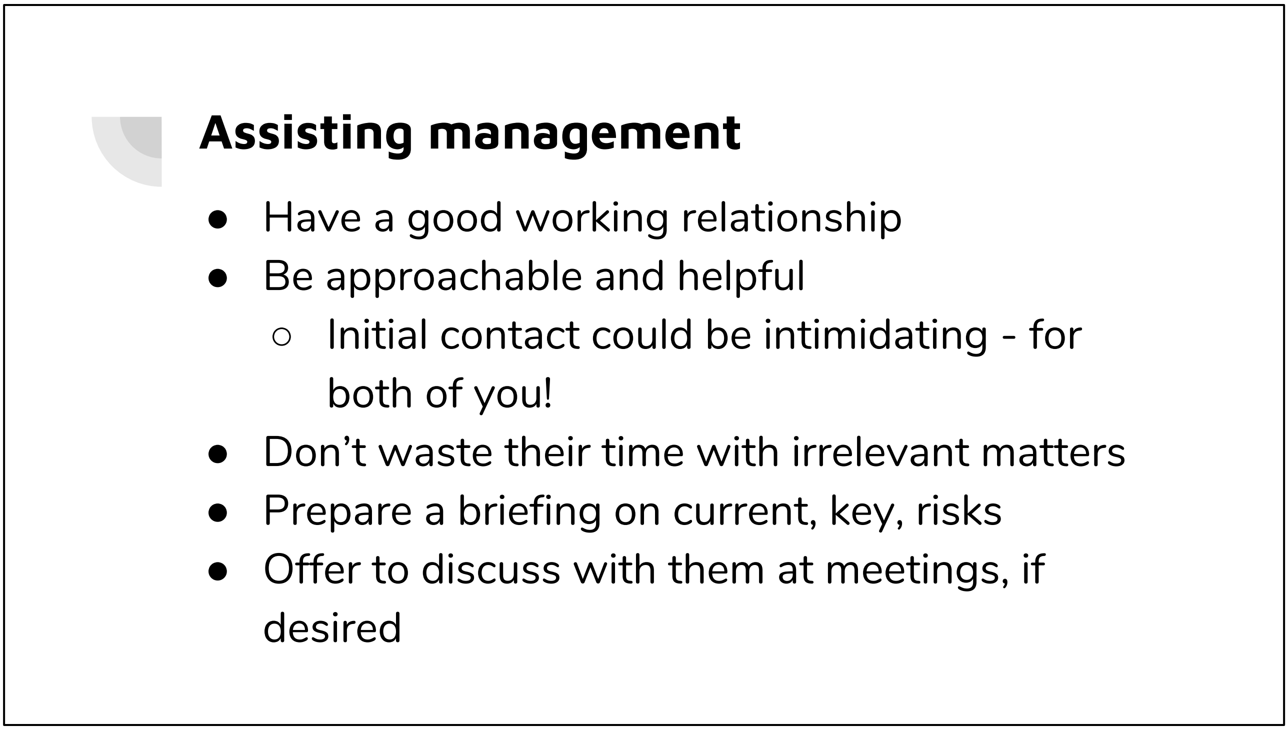
Management

- Marketing material is often targeted at managers, and it’s persuasive
  - May not reflect reality
- IT managers may not be technical
- Other managers / board members likely need guidance
- Be wary of fear, uncertainty and doubt - media portrayals

We’ve likely all seen products that look really good in the marketing material, and security products are the same. Do due diligence on products and make sure they fit your requirements.

Establish yourself as an honest person that’s available to be approached. IT managers may not be technical and it’s almost certain managers / board members outside of IT won’t be, so be prepared to have conversations in a clear way and without jargon.

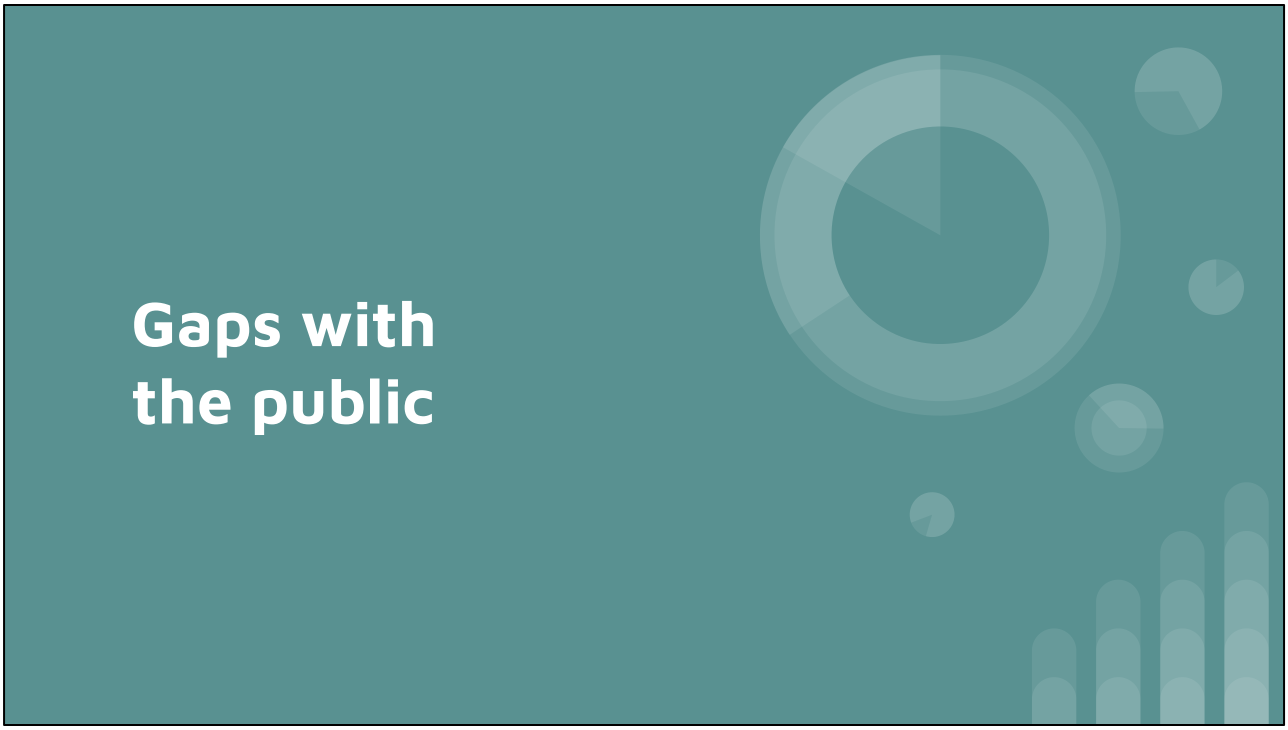
The media plays a big part in what people think is happening in the cybersecurity world - you may have to undo some misunderstandings.



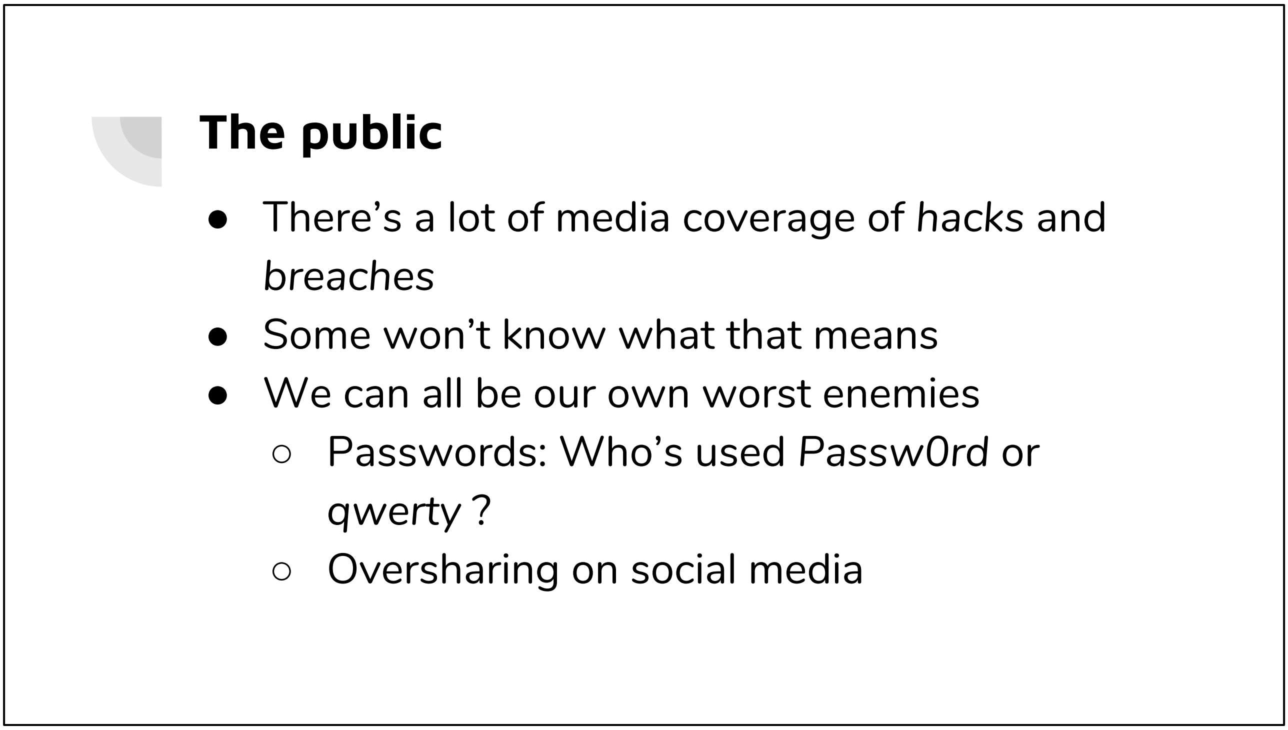
Assisting management

- Have a good working relationship
- Be approachable and helpful
  - Initial contact could be intimidating - for both of you!
- Don’t waste their time with irrelevant matters
- Prepare a briefing on current, key, risks
- Offer to discuss with them at meetings, if desired

Aim to have a good working relationship with the management team. Speak to them confidently but not arrogantly: they’re talking to you because the know they don’t know what you do. That can be daunting for both parties, so be respectful and you’ll probably find the management team will be too.



Gaps with the public

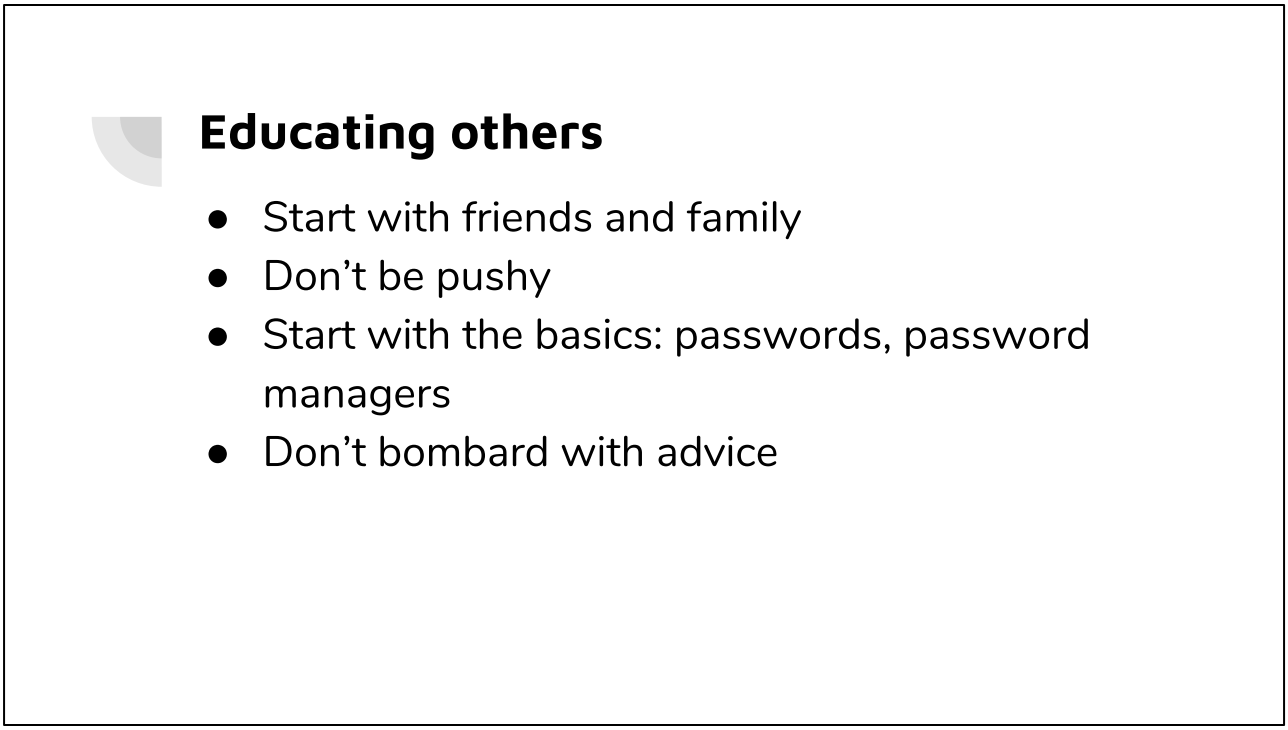


The public

- There’s a lot of media coverage of *hacks* and *breaches*
- Some won’t know what that means
- We can all be our own worst enemies
  - Passwords: Who’s used *Passw0rd* or *qwerty* ?
  - Oversharing on social media

Remember that you’re a member of the public too, just a (hopefully) better informed one!

There’ll be behaviours we all have that aren’t great for security. Oversharing on social media gives rise to a lot of privacy concerns.



Educating others

- Start with friends and family
- Don’t be pushy
- Start with the basics: passwords, password managers
- Don’t bombard with advice

Choose easy solutions as they’ll more likely be adopted. At the end of the day, changes to a person’s security stance are up to them, so don’t be pushy.

Thanks for listening

https://blog.jonsdocs.org.uk

@joncojonathan

https://uk.linkedin.com/in/jonathanhaddock

https://keybase.io/joncojonathan

Interested in security? Try a podcast

Smashing Security

Humorous run down of security news for the week. With Graham Cluley (@gcluley) and Carole Theriault (@caroletheriault).

SMASHING SECURITY

www.smashingsecurity.com

Security Now

A semi-technical dive into recent security news and vulnerabilities. Hosted by Leo Laporte and Steve Gibson (@sggrc).

SECURITY NOW
Steve Gibson

www.twit.tv/sn

Smashing Security is the less technical of the two, with episodes lasting around 45 minutes. Most episodes there's also a guest.

Security Now episodes tend to last around two hours.

Podcast logos © their respective authors

Acknowledgments and links

- Www icon
  https://openclipart.org/detail/216096/www-icon-black
- Keybase, LinkedIn and Twitter icons © their respective authors