GoVerify protects people from impersonation and deception fraud by validating the correspondence received from a trusted organisation is genuine without having to disclose any personal information.

GoVerify verifies calls, emails, texts and letters.
Version 2 – images not set as background, font coloured

All have the same content
Airline Travel Payment Summit, Fraud Conference

What should you be doing on the front line to help stop data breaches & managing the PR in the event of a breach
About Me

Co-founder and CEO of Appsecco
Passionate about helping people and companies be more secure
...buy my magic amulet and you’ll be fine, it’s medieval witchcraft, it’s genuinely medieval witchcraft.

Dr Ian Levy, Chief Technical Director, GCHQ’s National Cyber Security Centre speaking about the industry’s sales methods

Source: https://www.theregister.co.uk/2017/02/03/security_threat_solutions/
What we are covering today

We are going to cover
• Some common myths
• Some of the biggest reasons people get hacked
• So what?
• Simple things you can do if (when) there’s a data breach

We are not going to cover
• How much a cyber incident ‘could’ cost you when things go wrong
• Anything in-depth about technology and data security policies
• If you do want to get deep into this we’d love to hear from you, so connect through our blog - https://blog.appsecco.com/ or Twitter - @appseccouk
Myth: It’s a new thing

It’s been happening for longer than you think
The techniques used often aren’t new
Myth: Software & websites are built to be secure

Software developers aren’t usually security specialists
Simple mistakes can have unintended consequences
Myth: It’s an IT issue

Good security starts with everyone in an organisation. IT people support what you do, not watch over you.
Why hacks succeed

And thus data security is breached
There is always a trade-off.

Commercial pressure

Security

Time

Cost
Invisible supply chains

You

Development Team/Main Supplier

Onsite Freelancers/Specialist Partners

Outsourced Software Developers

Low Cost Software Developers

Individual Contractors
So what?
How does knowing this help me stop a breach?
You don’t know where the weaknesses are

“It’s only test data” (that was recently live data)

‘Island Hopping’ could account for 25% of losses by 2024

Source: Accenture’s Technology Vision 2019 report
You may not know who to ask to get good info’

Clear, timely and accurate communications are key

Who do you need to speak to?
The dead pharaoh risk

People don’t generally like being the centre of attention
This probably applies today and definitely when things go wrong
What can you do?

Any change you make is better than doing nothing
Get stuff checked now

Start asking questions so that this is on someone’s radar
Think about all the places where data could reside
Low hanging fruit is a good cliché
Have a plan (and test the plan)

Plan for ‘when’ not ‘if’

Make sure everyone expected to be involved knows ahead of time
Communication is more than a press release

All communications, including internal, will become public

Think holistically
Learn how to talk to techies

A direct question will often get a direct answer

Explain what you need to achieve and why
What should my next steps be?

- Conduct external audits and quickly fix any obvious problems
- Ensure someone understands your entire supply chain and the security standards they work to
- Figure out who you’ll need to call and start making friends with them today!
Questions?

gwilym@appsecco.com