SANS European Security Awareness Summit 2017

Handout notes for “Turn sceptics into advocates”

David Porter, Head of Innovation, Information Security Division, Bank of England

A brick wall

So there you are, a cyber security professional, presenting your security pitch to senior business managers. You’re the expert, you know all the right words and you have a killer solution in mind. This can’t fail.

But you end up hitting a brick wall. Despite your hard work, the message just isn’t getting through and you don’t know why. And you find yourself wondering what on earth will it take to turn sceptics into advocates?

The context

Let’s set the scene. At the Bank of England, for the past three years, we have been executing a supervisory programme called CBEST. This is an intelligence-led penetration test against a firm’s live critical computer systems. As well as testing the firm’s defences we also assess how quickly the firm detects and responds to the attack.

CBEST is underpinned by three key deliverables. Firstly the Targeting Report which reveals how much confidential information a firm is leaking online. Then the Threat Intelligence Report which reveals which threat actors present the greatest risk to the firm. And finally the Penetration Test Report which reveals how successfully the penetration test team penetrated the firm before they were detected.

Now it’s essential that senior management understand these reports and the principle of the test. So how have we avoided hitting that brick wall? How have we turned potential sceptics into advocates?

Make it visual

Well, the first rule is to keep it visual. The Targeting Report, for example, contains a huge amount of words, many of them technical which the Board won’t understand. We need to hit them with visual images to drive home our messages.

One method is to forget about words and instead produce a rich graphical overview of the key information we have discovered on the open Internet. This really grabs people’s attention and makes them want to know more — especially if you bring a big printout and unroll it across the desk.

Sometimes a picture is worth a thousand words. People who work for organisations often post photographs of their workplaces on social media not realising the risks they are taking. Showing your readers these kinds of photographs reinforces the point that seemingly innocuous information of information can be of huge value to criminals.

Keep it simple

Cyber security experts need to keep their writing as simple as possible. It is easy to write large quantities of dense, clumsy, badly structured sentences but harder to be concise. Consider this example from a real-life security report:

“Using our approach and this way of working we have achieved an end-to-end 100 day solution implementation timeframe to an initial release for this type of security scenario.”

What on earth are they trying to say? Perhaps they mean:

"Using this approach we built a first version in 100 days."

If that's what they mean then why not just say it? Unfortunately many information security experts, particularly technical ones, think that they need to write complex sentences since they are talking about a complex subject. Many do it because they want their writing to sound important and compelling. But it's a big mistake. Keep it simple otherwise the reader will turn off.

Aside from being more concise, there are some tricks we can use to hugely improve our report writing. Consider this text:

"A range of security recommendations is proposed by Information Security, from quick wins through to major initiatives. Information Security would discuss these with the Operations team after the report has been delivered."

While there is nothing fundamentally wrong with this paragraph it could be hugely improved with just a few simple changes:

- *"is proposed by Information Security"* is a very passive way of writing. *"We have proposed"* is more active and assertive;
- *"Information Security would discuss"* uses a conditional form which can come across as weak. And it sounds impersonal. *"We will discuss"* uses the future tense and is much more assertive and personal;
- *"The Operations team"* sounds impersonal. *"You"* is much more personal and engaging;
- *"the report has been delivered"* is, again, a weak passive voice. *"We have delivered our report"* sounds so much stronger.

So here's the finished piece for you to consider:

"We have proposed a range of security recommendations, from quick wins through to major initiatives. We will discuss these with you after we have delivered our report".

Three simple changes — active voice, personal pronouns and future tense — can make all the difference.

Tell a story

Security awareness professionals often use storytelling as a device for raising user awareness. We've also found it invaluable for describing complex subjects like CBEST cyber attack scenarios.

Take any good book, play or movie and you will see that the story usually unfolds using the classic story arc. A scene-setting exposition, involving some complication that needs to be resolved, followed by some rising action that leads to a climax which is then followed by some closing action and a final dénouement to wrap things up.

In CBEST we describe cyber attack scenarios using the same kind of narrative structure. We effectively turn the test into a story. We begin by setting the scene: the state of the world and the target and then introduce the threat actor, their goal and their capability. The story gathers pace as the attackers (testers) undertake reconnaissance and prepare their attack vectors and then reaches a climax as they infiltrate and retrench within their target's computer systems. The closing action revolves around the attackers compromising the target in some way and then exploiting the compromise. And finally we have the dénouement that describes the impact of the attack on the target and the threat actor's strategic follow-up to the attack.

This kind of narrative is more intuitive and engaging than a dry, scientific technical report. A story-based structure also allows for an easier arrangement of fixed information and demarcated spaces for improvisation.

Final thought

The film director Alfred Hitchcock always used to refer to a device he used in his films which he called the "McGuffin". When he was once asked what this was he replied: *"A McGuffin is nothing at all".*

A McGuffin is something you will find in most of Hitchcock's films. It might be a piece of microfilm, a priceless diamond necklace or a top secret formula. To take a more recent example, it might be the fictional mineral Unobtaineum which was featured in Avatar. Whatever form it takes, the McGuffin is a plot element that motivates the characters. But the McGuffin is NOT the plot. Usually the audience never actually gets to see a McGuffin and by the end of the film they don't care that they haven't.

But when cyber security people try to tell a story their McGuffins – cyber buzzwords like *zero-day exploit, kill chain, APT, TTP, endpoint* and *IOC* – take centre stage and try to be the plot. They should fade into the background where they belong but this rarely happens.

And so we end up hitting a brick wall and wonder what it will take for our message to get through. The answer is simple: make it visual, keep it simple and tell them a story. This makes what you have to say interesting to your audience. And an interested audience will understand anything in the world.

Further information

Please contact: david.porter@bankofengland.co.uk