Cybersecurity - Training your staff.

Taz Wake | Halkyn Consulting Ltd | Originally published 2024-05-30

Disclaimer: I teach digital forensics and incident response classes for SANS, a cyber security training provider. I am not paid to write any blog posts though.

Introduction

Cybersecurity is significant for any organisation with one or more devices connected to the internet. Even if you dont have a formal CISO or "*Cybersecurity*" team, you need to do cybersecurity or, eventually, something bad will happen. I dont mean this in the end-of-the-world way some people suggest - if your turnover is £100k, it is unlikely a breach will cost you £100m. But bad things will happen.

Background

There are lots of ways you can defend against this, but they really boil down to one of two strategies:

- **Spend money on technology**. You can absolutely throw huge sums of money at this problem if you want. There are cybersecurity tool vendors who will sell you pretty much anything.
- **Spend money on your staff**. Alternatively, you can invest in hiring good people, retaining them and making sure they are well-trained.

Which should I choose?

It really is up to you which path you go down, but to set the scene, I want to borrow a quote I first heard from the awesome Mathias Fuchs:

> "*A fool with a tool is still a fool*"

This is pretty important to remember.

If you have poorly trained, poorly paid and unmotivated staff, spending £100m on the best security tools in the world will not have a positive result. You can't tool your way out of bad staff.

The opposite, however, isn't true. If you have well-trained, well-paid, well-motivated staff, it won't matter what tools you have. They will do amazing things with completely free software.

There are always some concerns around this but they generally boil down to budget and retention.

While it is true, that retaining good staff can be expensive, so is buying good tools. For example, you can spend £2m a year on a tool, or hire 5 incredible analysts for £500k a year... We occasionally trick ourselves into thinking CAPEX and OPEX matter here, but they really don't.

What else do I need to consider?

The other worry is retention. The famous quote (attributed to Henry Ford) is good here:

> *The only thing worse than training your employees and having them leave is not training them and having them stay.*

Retention can definitely be an issue in cybersecurity. Some roles have incredibly high turnover (SOC analysts, for example) and across all the cyber roles, staff generally hop jobs every 3-4 years.

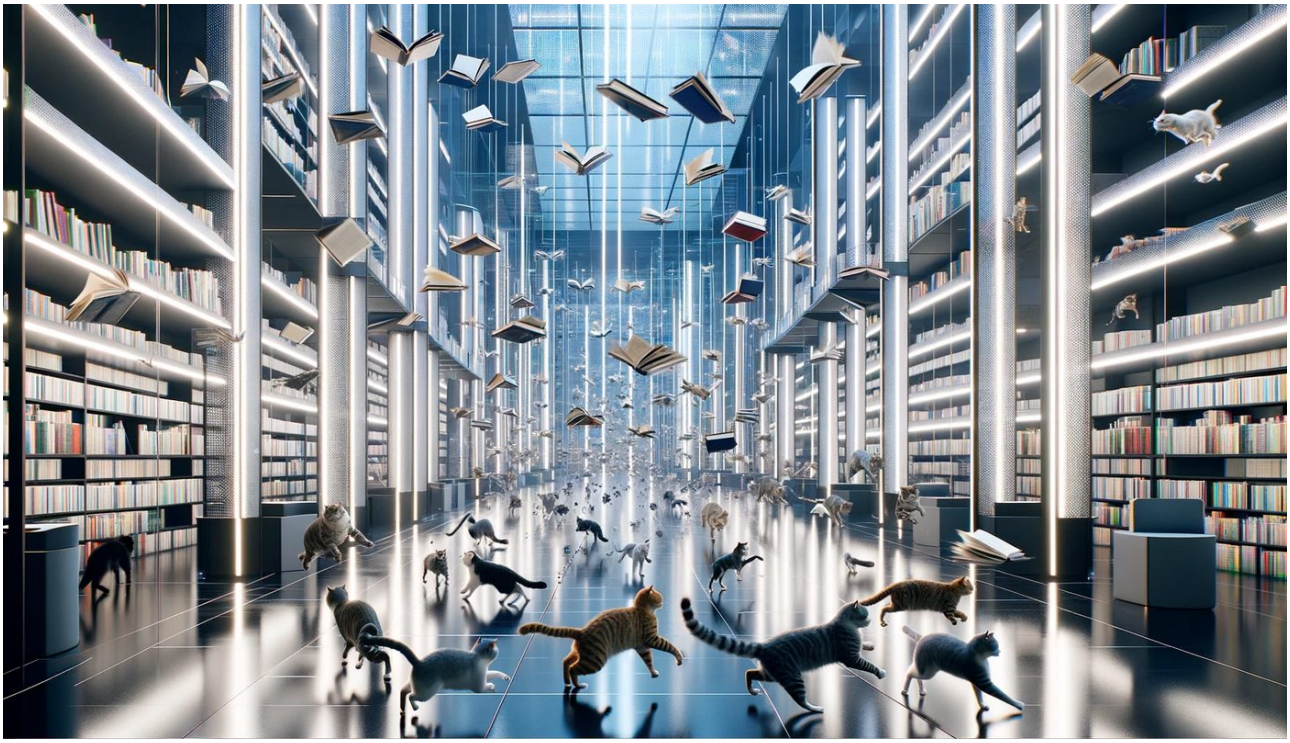
But, interestingly enough, retention is surprisingly easy to address.

- Pay your staff the correct rates for the job - not market rates from 2010 because that's what you remember.
- Train them to excel in their jobs - "Investors in People" was created for a reason.
- Give them work that makes them feel valuable - remember they want to do the job they applied for, not random other work.
- Provide a career path - this is critical, people need space to grow.

The hard part is actually delivering that in an organisation, but that will have to be in a future article.

Ultimately, training your staff is a significant part of what you need to do in order to retain them. Cybersecurity is a constantly evolving environment. If they knew good stuff when you hired them, 2 years later it is going to be much less relevant and useful.

This means you have another simple choice. Train your staff and make sure they remain effective or dont train them and let their skills and knowledge age out. For all his other faults, Henry Ford was correct on this.



Training

Now we agree that training is an essential part of building a strong security defence, the next question is how to determine what training people need.

Options

There are several approaches you could consider here. The three most common are:

- Carry out a formal job evaluation and determine what skills are needed for each role within your organisation. This is very, very effective and will provide you with well-targeted training requirements. However, it is very time-consuming and can be incredibly resource-intensive (people and money). This is not for the faint-hearted and likely only works well in a few organisations.
- Let your staff decide what they need and just set a budget for them to draw against. This feels the most employee-friendly, but it comes with issues. First, your employees *might not know* what skills they lack because it is hard to know what you dont know. Also, it is harder to get any feeling of ROI because there are no strong guides as to what they should know. For example, is paying £1000 on a kilt weaving course a worthwhile spend for a SOC analyst? Finally, how do you decide what the budget should be? It creates a lot of circular reasoning which can be difficult to get out of.
- You can use a publicly available pathway or framework - such as NICE or SANS which says things like people in job X should have skills Y. This is much easier,

certainly, but is often very generic. It is hard to know if they are really relevant (*do you need a CISSP to be a pentest lead*?) or if they are what your staff **actually** need.

As you can see, they all have strengths and weaknesses. There is no ONE TRUE WAY to deal with this.

Other considerations

- Your staff are not always the best people to decide what training they should have. I've been in sessions where a manager has asked their staff "What training do you think you need for your job" and the team have panicked, thinking that it implies they cant do their job and said "Nothing."
- Once you have a trained staff, training becomes a retention issue. One-off training is significantly less effective than having a training plan for your team. Everyone needs refresher training, new skills and to learn interesting things.
- Give people the chance to learn new things and you get new ideas, new skills and can go in new directions. Send your detection engineers on a reverse engineering course and they will have new ideas on how to detect attacks. Send your threat intelligence people on a vulnerability management course and they will have new ideas about how they can relate their work to the stakeholders, etc.

Training types

- **Paid Training**. This is the easiest to plan for. You put aside a budget, allocate time for your staff, and they go on the training. Everyone benefits. The biggest issue here is normally the cost.
- **Free training**. This seems attractive but the quality can vary massively. Some of it can be amazing, but some of it can be dated, irrelevant or incorrect. With free training, you still MUST give your staff time to study. If you expect your staff to study free material, in their own time, dont be surprised when they leave you.
- **In-person**. I am using this to mean live training where you travel to a place and have someone teach you the material along with other students. For most people, this is the best way to learn as you get the chance to ask questions, read the instructor's body language and interact with other students. A significant amount of learning comes from discussions with other learners.
- **Live Online**. Here I mean you are on a live course but have accessed it from a remote location. This allows you to study with an instructor in real-time from anywhere in the world. It does lose some of the social interaction but this can be a benefit for people who find that tiring or difficult.
- **Self-paced**. By this, I mean training where you are given access to all the material and study at your own pace, wherever you want. This can be excellent if you need to fit study around other commitments but be aware that it can also be very hard to force yourself to put aside enough time to learn the material. If you are sending your staff on self-paced training, you really should allocate them a lot of study time during working hours.

The best approach is to find a combination of things that work for each individual. Everybody learns in different ways, so try to avoid taking a very prescriptive approach for an entire team.

Ideally, look to offer a range of options so each person on your team can achieve their learning goals in the best way for them. For example, I learn best in formal classroom-type settings, other people do much better sitting on their own, reading at their own pace.

Summary

- You really do need to train your staff. Spending more here will allow you to save money elsewhere. Only invest in tools, once you have skilled staff.
- Investing in your staff will help recruitment, retention, and lower costs. It is a good investment. It is almost never wasted.
- Your staff will have wildly different training needs. Try to tailor it to them, not an arbitrary idea of what they should like.

This is simple stuff, but it is often overlooked in many organisations.

About Halkyn Consulting

Halkyn Consulting Ltd is a UK-based security and risk management consultancy providing 24/7 incident response, digital forensics, threat hunting, virtual security leadership (vCISO) and security compliance support to organisations worldwide. We deliver clear, practical, vendor-independent advice based on real-world threats — no hype, no upsell.

More free security resources are available at www.halkynconsulting.co.uk/security-resources.

Web: www.halkynconsulting.co.uk | **Email:** info@halkynconsulting.co.uk | **Tel:** +44 1244 940858