

FIT Remuneration Consultants talk about why and how they build cyber security resilience.



Who did we interview?

John Lee · Managing and Founder Partner

FIT provide Focused, Independent and Tailored executive remuneration consulting. They advise organisations on all aspects of remuneration, from benchmarking through policy design, shareholder consultation and legal implementation. FIT works closely to ensure its solutions align closely with each client's strategy. They are founder members of the Remuneration Consultants Group, responsible for the sector's Code of Conduct.

Many firms struggle with cyber security because it's too technical or complex, or they believe themselves not to be at risk. How does FIT think about cyber security?

I understand some reluctance regarding security spending, but generally, preventative spending is lower and less stressful than corrective action.

The logic we follow is that the data we hold is sensitive and important to clients, so we need to do our best to protect it. The idea that we are a smaller firm and should, therefore, be held to a lesser standard doesn't make sense. Smaller and larger organisations must both demonstrate that they take adequate precautions.

How do you make decisions about cyber security?

In 2011, we looked very carefully for a technology company with whom we could partner. We've worked with The Final Step since then. We wanted a company that shared our values and proactively told us what we should think about. We need advice on what good security looks like and what best practices are appropriate for us and our clients. Due diligence, legislation, and the news will often raise areas of concern without necessarily providing solutions.

Despite being a small company, we believe we have a best-in-class cyber security system, and we're advised by The Final Step, a similarly small company.

How has your thinking about cyber security changed?

Since the implementation of GDPR, we have spent much more time thinking about data protection and cyber security. Covid produced another significant change in our security mindset. We became more aware that security is only as good as your weakest point, and new hybrid working trends have opened up more security gaps.

As risks change and evolve, we regularly review and, when necessary, add extra layers of protection. We also evaluate certifications as a methodology for maintaining good standards and demonstrating that we take security seriously.

How do you set budgets for mitigating cyber risk?

We tend not to impose initial limits because we want to hear what we need to hear. But we live in the real world, and that is tempered by regular meetings with Steve Anderton, our advisor and dedicated contact at The Final Step. We really value the continuity of service, and we meet annually to set a budget and roadmap and then two or three times a year to verify those plans.

These meetings and the current environment's context define our budget and give us a prioritised plan. Over the years, we have got to know each other well, and The Final Step bases its recommendations on which investments will have the most impact. We spend more on IT now than before, but that is required.

Why did you commit to Cyber Essentials Plus certification?

We consider certifications because we primarily deal with larger companies with procurement processes that ask a wide variety of due diligence questions. Cyber Essentials Plus shows that we are committed to specific standards and reach and maintain them year-on-year. That is very reassuring and, in some cases, required of us.

However, certifications only satisfy some due diligence questions. Often, we turn to The Final Step to help us fill out forms and offer more detailed explanations. Steve is very responsive and integral to our procurement fulfilment process.

What's important to you in a security partner?

What we want in a partner is a sense of shared values, trusted and relevant expert advice, and a commitment to a long-term relationship. We don't want to make changes in this area too often.

Any firm is only as strong as its weakest link. We think of The Final Step as part of our extended team. We appreciate the planning and responsive support. Your speed of response is good in all areas of support you provide, not just cyber security. It's rare that someone doesn't deal with our requests straight away.

You are quick and you care; you see any problem we have as your problem, too. That is really valuable. You provide excellent service, and we've never felt the need to look elsewhere. We are very happy customers and have been well-treated throughout our partnership.

One of the reasons we provide high-quality service is that we don't have to fret about back-office IT or cyber security, because we know we have someone who looks after us from that perspective.

If you feel your business would benefit from someone looking at it through a cyber security lens, please get in touch for a consultation.

We offer a risk assessment customised to your business and circumstances. From that, we can create an action plan prioritised to mitigate your most significant risks, based around an annual budget.