

# Human error: Your biggest cyber security risk



Why cyber security awareness training is so important for you and your staff



Author  
James Tilbury, CEO

# About the author

**James Tilbury, CEO, ILUX**

James is a graduate in Computer Science specialising in software engineering. He has worked in various IT-related roles, including a global healthcare manufacturing business supporting the systems and infrastructure.

IT is part of James' DNA. His father founded Tangerine Computer Systems, who developed the TAN1648 VDU kit and the Microtan 65, a forefather of home computing in the late 70s.

James has worked around the world, both in a software development role and performing major infrastructure enhancements and is widely recognised as one of the leading experts in digital transformation.

Having identified a need for enterprise-quality IT support and project management for SMEs, James founded ILUX to focus on IT supporting business growth.



## Imagine the scenario...

The invoice seemed routine, nothing out of the ordinary. There was no need for concern when the CFO emailed the accounts team to request urgent payment, reminding them of the importance of their relationship with a supplier. The email also mentioned they recently changed banks, so it would be greatly appreciated if you could kindly update their details accordingly...

Given that it is a small company where everyone is familiar with each other, there were no apparent warning signs.

However, something was definitely wrong. The unfamiliar payment details actually belonged to a criminal gang. The email did not originate from the CFO.

This marked the final stage of a highly sophisticated phishing scam known as CEO fraud, and unfortunately, it has resulted in a substantial loss for the company.

The cyber criminals managed to gain unauthorised access to the CFO's email account, intercept a message, and maliciously alter the information to redirect a payment.

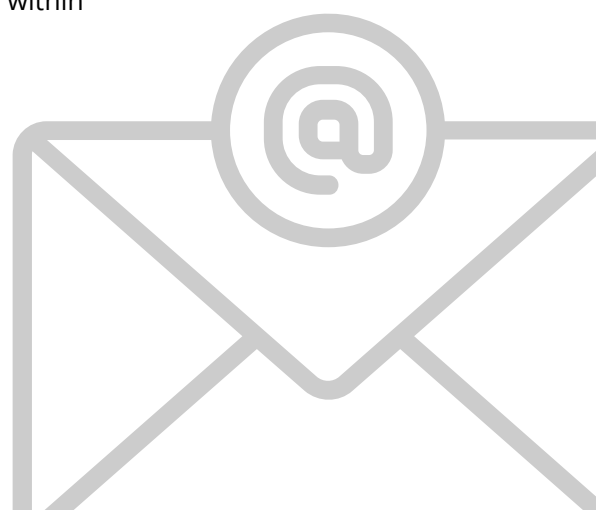
As is often the case with cybercrime, it was a simple human error that allowed the criminals to succeed. No one was aware of the signs indicating that something was wrong, and no existing policy required individuals to personally verify payment requests when there were changes to be made.

This incident was financial fraud. However, these criminals were not solely interested in the organisation's money; they also highly valued the business data and are happy to go to great lengths to obtain it.

Small and medium-sized businesses are particularly vulnerable to various types of cyber attacks and not limited to phishing scams like this one. Cyber criminals are aware that these companies often have weaker security measures in place and often don't invest as much time in training their staff.

It is crucial to recognise that your employees are the weakest link in your security chain, not because they have malicious intentions but simply because they are human.

Without proper training, they may be unaware of the risks to watch out for and how to safeguard your business. This underscores the importance of comprehensive cyber security awareness training for all employees within your organization.





# Find your baseline

Your training sessions need to be complicated and lengthy, but preparation is everything

Start by working out your team's awareness levels and where you may be exposed to security threats. It is an important part of the process and may open your eyes to some surprisingly risky behaviour.

You need to find the baseline level of staff's cyber security knowledge – some people may be starting from zero. And if you know that your knowledge has gaps, this is the point to seek professional help.

Examine the way everyone works to understand which behaviours are a threat to your business. There are countless kinds of cyber attacks to protect against, so you need to be systematic in your approach.

Look at:

- Emails, communications and file sharing
- Logging-in behaviour
- Attitudes to policies around data protection and information handling
- General awareness of cyber threats

Every business is unique, so prioritise according to your needs.

Observe their behaviour rather than simply assuming that policies are being followed. This will give you the best idea of where your vulnerabilities lie, and help shape to your training sessions.

# Assess the risks and prioritise

Your audit will give you an understanding of your team's security behaviours. Prioritise your training programme to deal with the most pressing risks first.

There are security threats on many fronts—Prioritise training on the most immediate weaknesses, dealing with any obvious knowledge gaps first.

Risk assess your current systems, your network, and your digital assets. Look also at who has access to what information and why.

# Re-assess as you go

If you deal with sensitive data of any kind, take this opportunity to look at your wider policies alongside your training plan.

A zero-trust security policy may be appropriate for you. This means that only people who need access to sensitive information can – everyone else is locked out.

These assessments will help you create a training programme tailored to the right people and pitched at the right level according to their roles and responsibilities.

For example, a warehouse fulfilment team may have access to private customer address information. That requires a different security awareness to an HR manager with access to sensitive staff health records.

# Create your training plan

Once you've got to grips with the needs of your different employees and the wider business, match them with the resources available to you to create a training plan.

Lay out your objectives – the skills and knowledge you need to develop – and the attitudes and behaviours you need to see at work.

Then break each objective down into topics or modules. For example, there may be a module on phishing emails and one on data classification (where your data is grouped according to how sensitive it is – staff sickness records, customer financial information, sales process documents).

Sessions can be online or in-house; where possible, training should be interactive and hands-on to help people retain information. Reading a guide or completing a workbook alone is unlikely to help someone understand and retain what they've learned. The training should be enjoyable even though the subject is a serious one.

Continually reinforce the consequences of how any data falling into criminal hands can be disastrous for your organisation. That's why when everyone has completed the training, there should be clear repercussions for anyone who doesn't put that training into practice.



# Begin training

Explain exactly why the training is being introduced, the range of threats faced by the business, the desired outcomes, and the benefits both to employees and the company.

You may host all of the training yourself, but it is good practice to use outside expertise. Not only will this save you time, but also reassures you and the rest of the organisation that the training is comprehensive and that training materials are current.

The training provider should work with you so that everything you have identified in your risk assessment is included and suggest any additions.

Remember that the training should be for everyone in the business. It should become part of your employee onboarding package and part of the transition process when people change roles.

If you have an IT support partner, they may offer this type of training and will be familiar with your systems.

If you don't have an IT expert on hand, get in touch with us, we'd be happy to recommend some training or could develop bespoke training for you.

# Put it to the test

When you've invested time and money into training, you want to ensure it's doing its job.

Occasional tests and quizzes are an option, but the most effective way to find out if your people have used their training is with a simulated phishing attack. Platforms can help you do this, but you can also do a lot yourself.

A simple phishing simulation might involve sending everyone an email with the intention of tricking them into taking action. It could invite them to click a link for a gift card as thanks for their hard work or ask them to reconfirm their login details.

You can see who takes the bait, who uses their training to spot the scam, and who takes the required action.

Other training and testing methods include interactive phishing training with online applications that work like chatbots and even testing that takes the form of a game to make it more engaging and interactive.

Think of it like a fire drill. The key is to avoid warning your team a test is coming. You don't want them to be on guard. Further training may be necessary for those who don't pass the test.

# Create new policies

If you don't already have a cyber security policy that sets out your expectations, it's time to create one.

Your policy should be detailed but easy to understand. Describe the security controls you have in place and the threats they address. Include who is responsible for maintaining them, how incidents should be reported – and who to – and the consequences of not reporting a potential cyber security risk or attack.

Highlight your expectation that your people should use your security measures, follow protocols and use best practices at all times. Again, include the repercussions if someone knowingly fails to do so.

Include a remote access policy, acceptable internet use policy, and information about managing updates.

You could also consider a section on personal devices used for work purposes and how they should remain secured to protect company data.

Most people in your team will take protecting the company and its data seriously. But there could be individuals that may not. Enforcing your cyber security policy will ensure everyone recognises its importance and the serious risks you protect the business against.

When things are laid out clearly to employees, they'll feel more involved and more motivated to help protect the business and understand the consequences of intentionally not doing so.

# Stay updated

Cyber security training is not a set-and-forget project. New scams and security issues always arrive, so keeping your people aware of what they should be looking out for is crucial.

Plan for quarterly or six-monthly refresher sessions for **everyone**, from your apprentices to the people on your Board. This ensures that everyone has the most up-to-date cyber security knowledge and reinforces the ongoing seriousness of the threat.

Between sessions, keep everyone updated on the latest cyber security news. Share news stories of significant data breaches, new malware and scams, and insights on your security measures. You can set up news alerts or take a weekly scan through tech news sites – it's incredibly worthwhile.

# Useful resources

Below are some free guides and links to cyber security training resources:

Prevent email scams -

The [ILUX Business Owners guide to Phishing](#)

How to achieve certification without the hassle -

The [ILUX Cyber Essentials guide](#)

Implementing password management -

The [ILUX MFA \(Multi Factor Authentication\) guide](#)

Keeping the cloud secure -

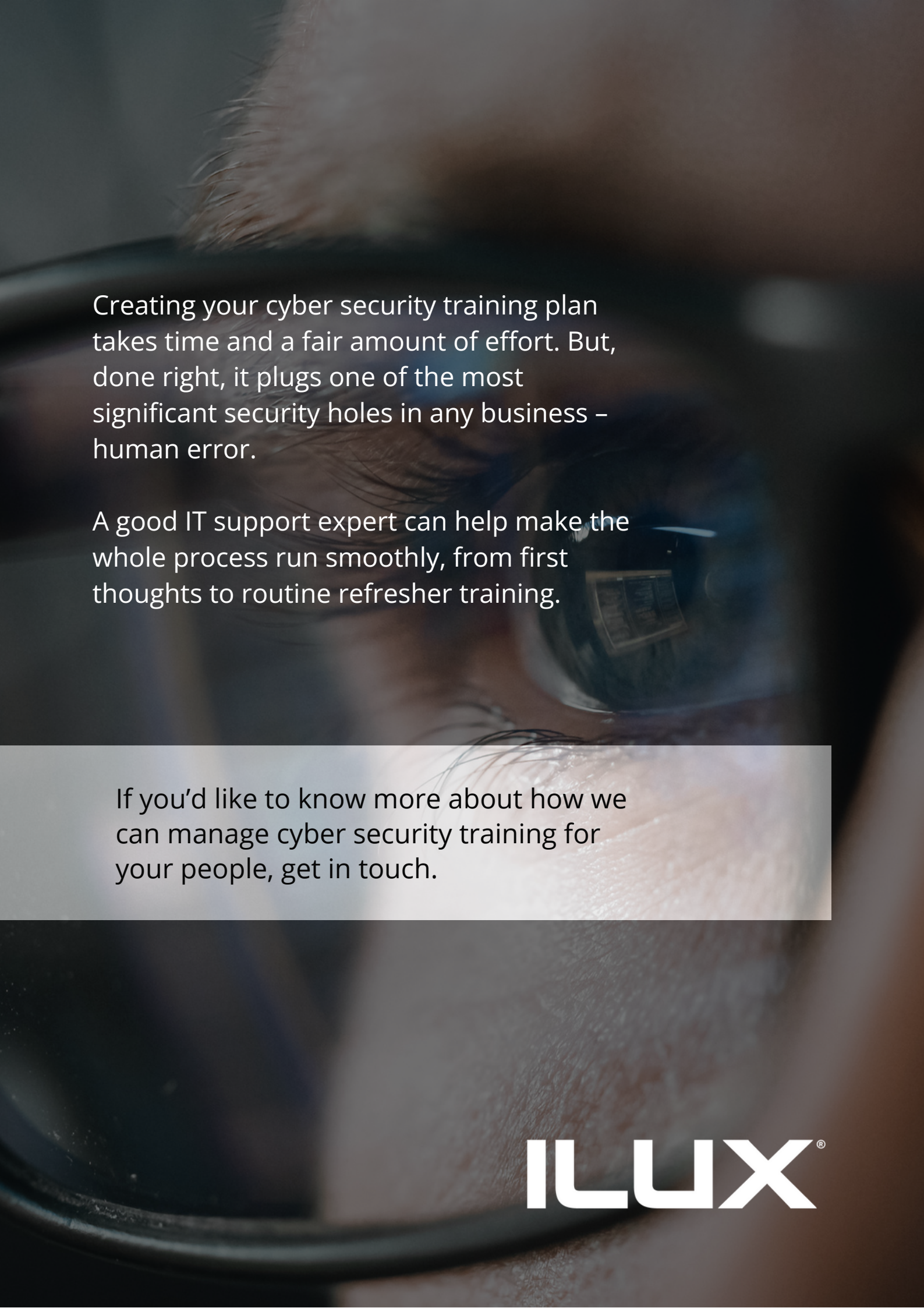
The [ILUX guide to Cloud Security](#)

Next level cyber protection -

The [ILUX guide to MDR \(Managed Detection and Response\)](#)

[Free online training for business from GOV.UK](#)

[Cyber security guidance for business](#)



Creating your cyber security training plan takes time and a fair amount of effort. But, done right, it plugs one of the most significant security holes in any business – human error.

A good IT support expert can help make the whole process run smoothly, from first thoughts to routine refresher training.

If you'd like to know more about how we can manage cyber security training for your people, get in touch.

**ILUX**<sup>®</sup>