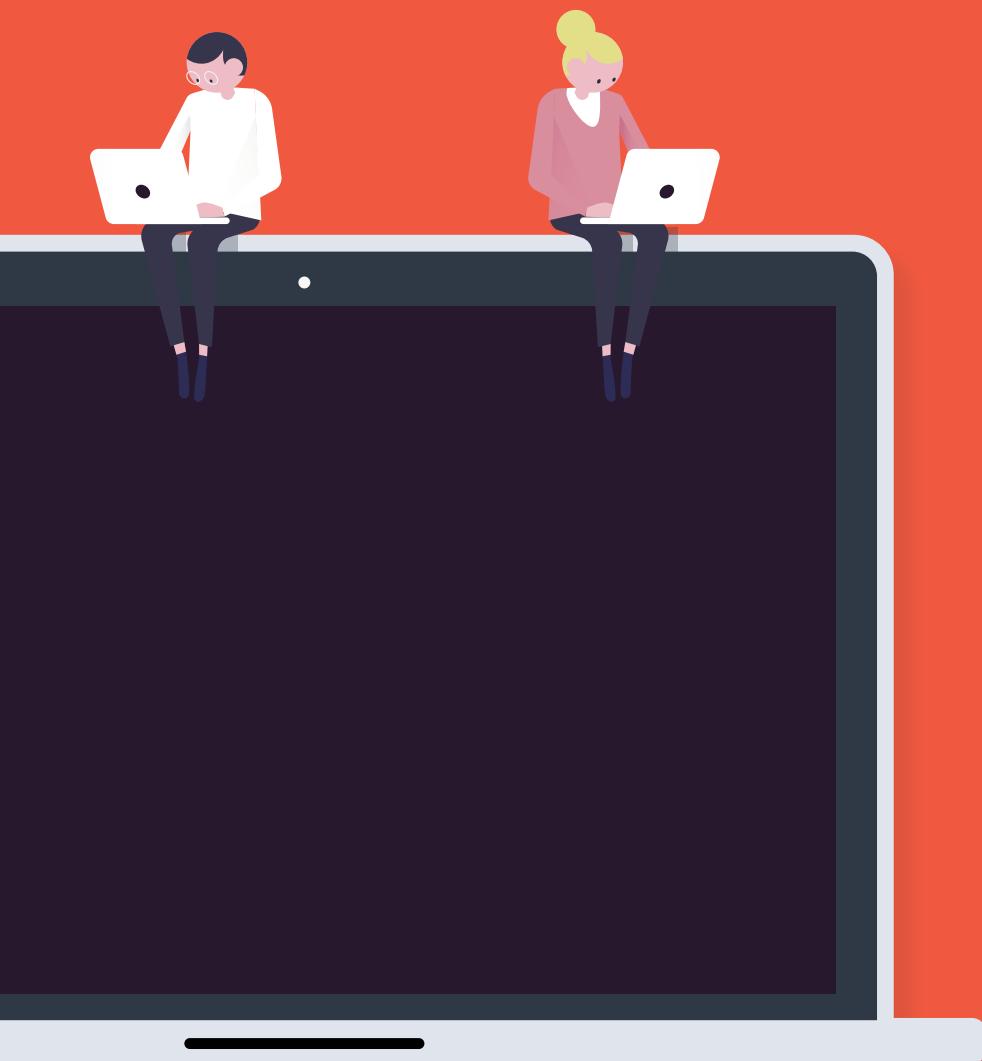


A hands-on guide to minimising this risk

Your employees are your greatest risk - not your IT



| Table of contents

PREFACE	3
Cultural change through four steps	4
<i>Cultural change in an organisation is a continuing process</i>	5
Information security threats occur and are solved from within	6
<i>The information security risk comes from within</i>	7
<i>The security solutions must also come from within</i>	8
#1 Clear communication is a precondition for success	9
<i>Clear Communication</i>	10
#2 Provide concrete guidelines	11
<i>Concrete guidelines pay off, literally!</i>	12
#3 Awareness above all	13
<i>Awareness is everything</i>	14
<i>Physical meetings or presentations</i>	15
<i>E-learning for awareness training</i>	16
<i>Awareness training in practice – what do customers say?</i>	17
<i>Phishing simulations</i>	19
<i>Phishing simulations - an example</i>	20
#4 Measuring is key	21
<i>Tracking your progress</i>	22
<i>Statistics from real cases – information security is still a great challenge</i>	23
Conclusion – achieve your goal of awareness	24
<i>The four steps to achieving awareness within your team</i>	25
<i>CyberPilot – your partner for information security and the GDPR</i>	26

| PREFACE

When you hear words like 'cyber security threats', 'cybercriminals', and 'security breaches' in organisations, not very many people realise that these problems can often be traced back to human error.

As a matter of fact, most information security breaches in organisations are because of human error. This can often be attributed to the lack of knowledge or awareness in the organisation when it comes to the secure handling of data in everyday work life. These can result in violations to the General Data Protection Regulation (GDPR).

In other words: **Your employees are your greatest risk - not your IT.**

The security breaches and data handling violations can result in severe financial fines. It affects organisations of all sizes and industries – even yours.

How should you counter these risks? Your organisation needs to create and maintain a culture that is based on the shared responsibility and awareness about information security.

The guide is based four steps, that you must focus on:

- Clear communication
- Concrete guidelines
- Awareness
- Tracking your progress

Enjoy reading!

CyberPilot

Cultural change through four steps

Cultural change in an organisation is a continuing process...

Creating awareness and maintaining good habits is a challenge and doesn't just happen overnight. On the contrary, it is a long process that takes initiative and a dedicated effort. It needs to happen on all levels of the company.

The change begins with management and works its way down to the team.

Initiating any sort of cultural change in an organisation can only be successful if those on the management level set an example. The goal is to get the new culture integrated seamlessly into the team's mindset when handling IT systems and data.

In order to reach this goal, the entire organisation must take four simple steps.

It is illustrated in this pyramid with four layers:



The process has four steps:

- **Clear communication**
- **Concrete guidelines**
- **Awareness**
- **Tracking your progress**

The pyramid illustrates the need for clear communication, **then** setting guidelines, **then** working with awareness, **and then** measuring the progress.

The process does not stop with the fourth and final step. Cultural change is a circular process that requires regular maintenance, improvement, and adjustment.

In the remaining part of this e-book, we will take you through the four steps and give you some inspiration on how you can begin and succeed in changing the culture with information security in your organisation.

**Information security
threats occur and are
solved from *within***

The information security risk comes from within

Before we dive into the four steps, let's first focus on the core issue: the information security risks.

In a digital age, where most, if not all organisations are dependent on IT systems and data, the risk of information security is more present than before. By default, we always blame external parties – hackers, scammers, and cybercriminals. We rarely stop to consider the role of our team in this context.

But consider this statistic:



9 out of 10 information security breaches in organisations start from within.

As surprising and disturbing as this number is, it also emphasises the risks that all companies and organisations face today.

The threat often comes from the little mistakes in the handling of systems and data. They can also occur when there are targeted attacks against the people in your organisation. Examples include phishing, social engineering, or scams which provide malicious parties access to your confidential systems and data.

Later in this e-book, we provide some statistics on how many people fell into these traps when we performed a simulated phishing attack on an organisation.

Spoiler: It is an alarmingly big number!

How do you even begin to counter this risk? We'll show you how...

The security solutions must also come from within

Because the threat arises within your organisation, the solution must also be found within, beginning with minimising human error.

The goal is to heighten your organisation's awareness and change habits by working with individuals. The change of culture means getting rid of the status quo and being open to change. Finally, the team should be shown how with learning materials and be given hands-on experience to enforce their training.

By incorporating new and safe habits in your organisation, you strengthen your team's ability to:

- **Be proactive in identifying potential risks** before they become harmful
- **Reflect and act rationally** in relation to information security
- **Discuss and communicate** clearly about mistakes and security breaches

These skills that will eventually lead to an increase in awareness, a reduction in errors, and most notably, a reduction in the security threat from within.

Let's have a look at the four steps that are going to secure you and your team's success and build concrete results.

#1 Clear communication is a precondition for success

| Clear Communication

The first step in your efforts to improve your information security is to clearly communicate the problem and effort to your team.

In organisations, changes are normally welcome but can also give rise to fear, insecurity, and doubt. People try to find comfort in the 'this is how we usually do it' attitude and might be resistant to change. Creating this change could become an even more difficult challenge.

In our experience, the best way to overcome this is to anticipate the insecurities and obstacles by discussing it openly and directly. This way, you prepare the entire organisation for the changes they are facing, which will mean that they are more accepting to change.

The result of clear communication means that your team will understand why the changes are needed and what benefits there are. Additionally, actionable steps should be provided.

Ultimately, what you communicate should clarify:

- What problems the organisation is facing
- What changes are going to happen
- What the benefit of the changes are
- What is expected of the team

Ultimately, this is about **managing expectations and communicating clearly**. This takes your team on board and prepares them for your journey together. Having said this, the change of culture can only be successful if management is supportive and strives to set an example.

If you would like some inspiration about how to address your team about their role in information security, feel free to contact us. Send us an email at info@cyberpilot.io with 'Communication' in the subject line to receive our templates.


#2 Provide concrete guidelines

Concrete guidelines pay off, literally!

Without clear guidelines, it will be difficult to know what is expected and enforcing good digital habits would simply not be successful.

That is why we recommend providing well-defined guidelines to describe what your organisation considers good practice. This means a clear set of rules that map out how to handle their digital activities in specific situations. We recommend making these guidelines accessible for your team to refer to.

Here are some examples of questions to answer to create clear guidelines:



	✓	✗
Is use of company IT equipment allowed for private use?	<input type="checkbox"/>	<input type="checkbox"/>
Do we allow the use of other applications for cloud storage? E.g., OneDrive or Dropbox	<input type="checkbox"/>	<input type="checkbox"/>
Do we allow the use of social media and what exactly do we use those platforms for?	<input type="checkbox"/>	<input type="checkbox"/>
Do we allow staff to install programs on their own?	<input type="checkbox"/>	<input type="checkbox"/>
Is it ok for staff to save files locally?	<input type="checkbox"/>	<input type="checkbox"/>

The idea is to provide what is needed to perform their jobs securely and with confidence. By answering these questions, you minimise the risk of error which may lead to fraud or crime.

If you would like to receive a template for some concrete IT guidelines, send is an email at info@cyberpilot.io with 'Guidelines' in the subject line to receive our templates.

#3 Awareness
above all

Awareness is everything. Create and maintain the awareness of information security in your organisation

One of the greatest challenges in information security is maintaining an adequate level of awareness in the organisation. Once you have provided guidelines and communicated your expectations, the next step is to focus on creating and maintaining the sense of awareness when it comes to information security and the handling of personal data.

Many organisations make the mistake of treating this as a one-off task. However, this often results in people forgetting it altogether. We recommend making a continuous effort to have information security as a priority on the long run. People need to be engaged to remember their good digital habits to maintain a high level of awareness.

There are many tools at your disposal to continually develop the awareness of information security in your organisation. We have gathered a selection of free and inspirational material in the form of templates to show you how to get started.

Suggestions to maintain awareness:

- Physical meetings or presentations
- Posters
- E-learning for awareness training
- Phishing simulations

In the next section, we will briefly describe each method for information security training.

Physical meetings or presentations

The first step in creating a culture of awareness is always the hardest. As a result, you need to make a substantial effort to launch your initiative. Physical meetings, presentations, or workshops have proven to be effective as a kick-off activity. They can also be tailored to focus on specific areas depending on your information security needs.

It can be a presentation at a provided by someone internally. Alternatively, it can be an external speaker or expert that is invited to the company to speak about information security.

The advantage of this is that you **activate and engage your team in person.**

At CyberPilot, we have compiled different types of inspirational material to share.

Feel free to contact us if you would like to hear more or receive the material.

Just send us a mail to info@cyberpilot.io with 'Awareness Presentation' in the subject line and you will receive the templates.

E-learning for awareness training

To be successful at creating a culture of awareness, it is imperative to maintain it in the long run.

Physical meetings normally require substantial resources in terms of planning, logistics, and implementation. Often, it is hard enough to get the entire team present, with perhaps some working remotely, off-site, or at a different office. Things can get even more complicated when new staff come on board; it would be difficult to ensure that everyone has received the same training.

While physical meetings *are* a good idea especially as a kick-off, it can be difficult to maintain the momentum over time with physical meetings.

This is why so many companies opt for e-learning for awareness training. E-learning is a smarter and more efficient way of ensuring that everybody receives the materials and is aware of information security - all without the inconvenience!

E-learning makes it easy to plan and carry out the training because your team can do the courses whenever and wherever they like. Additionally, the awareness training can be tailored to the needs of each person on the team.

If you would like to test our awareness

training or if you are looking for inspiration for your own awareness training course, you are welcome to try CyberPilot's awareness training. It covers information security and the GDPR.

[Try it for free](#) and 100% with no commitment.

Awareness training in practice – what do customers say?

What do you get from e-learning for awareness training, and does it work? We'll let our customers tell you.

"I was surprised when a couple of employees, who were shortly into the course, came down to the IT department suggesting that we use two-factor authentication more extensively in the company. Previously, it has always been a struggle to even make them change their passwords! In general, I feel that the employees no longer just think that IT security is a nuisance. They do understand the importance of it."



Jesper Christensen
CFO at Dacapo Stainless

"CyberPilot's awareness training covers our needs for the continuous training of our team."

Lars Juul

Head of IT at EUC LilleBælt



"We use CyberPilot as an external sparring partner for cybersecurity, vulnerability scans, and awareness training. We have always received constructive and qualified help."



Lotte
Uniconta

"You're onto something very important – awareness training is for EVERYONE."

Tina Britting

Head of IT at EUC Sjælland



"CyberPilot's presentations provide a quick overview of various cybersecurity topics that many of our teachers and secretaries are pleased with. Some learn something new and some refresh their knowledge. The best part is that everyone can do it at their own pace and at any time. Since GDPR requires a cybersecurity course for all employees, this has been a great help. It is especially helpful to be able to get a scheme that fits perfectly into my safety strategy for the employees. I was able to browse through the entire course catalogue and even enrol in all the courses that I thought were relevant. There is a lot of flexibility, which is good for such an extensive topic"



Bente

Favrskov Gymnasium

"Simply put, we have not had any security breaches since we started the awareness training"

Rune Udby

CFO at Firtal



"Cyberpilot's awareness lessons are written in a language that everyone understands, making it easy to relate them to the situations we face daily. This makes you remember what you are taught when you need it. Additionally, the lessons are short and easy to fit into a busy day. Our experience is that our team now shares a lot more information about how they have discovered and rejected phishing emails. The lessons live up to our expectations 100%"



Jacob

Danish Fashion and Textile

| Phishing simulations

The fourth tool we want to present is phishing training. Phishing is the greatest threat when it comes to it cybercrime today. As mentioned earlier, **9 out of 10** attacks begin with a targeted attempt to hit the organisation through their team. Providing guidelines, courses, and e-learning are good ways of drawing attention to the red flags and suspicious activity.

However, we have found that nothing beats real-life experience – that is, handling a ‘real’ cybercrime attack. We often recommend that phishing training is carried out as a separate measure, so your team can see how they handle themselves when they are faced with a phishing attack.

In short, phishing training is about exposing your team to simulated phishing attacks with the goal of:

- Testing team’s preparedness
- Creating even more attention about this threat

At CyberPilot, we work with organisations to create phishing training campaigns. You can read more about our phishing training [here](#).

“Simply put, we have not had any security breaches since we started the awareness training”

Rune Udby

Firtal

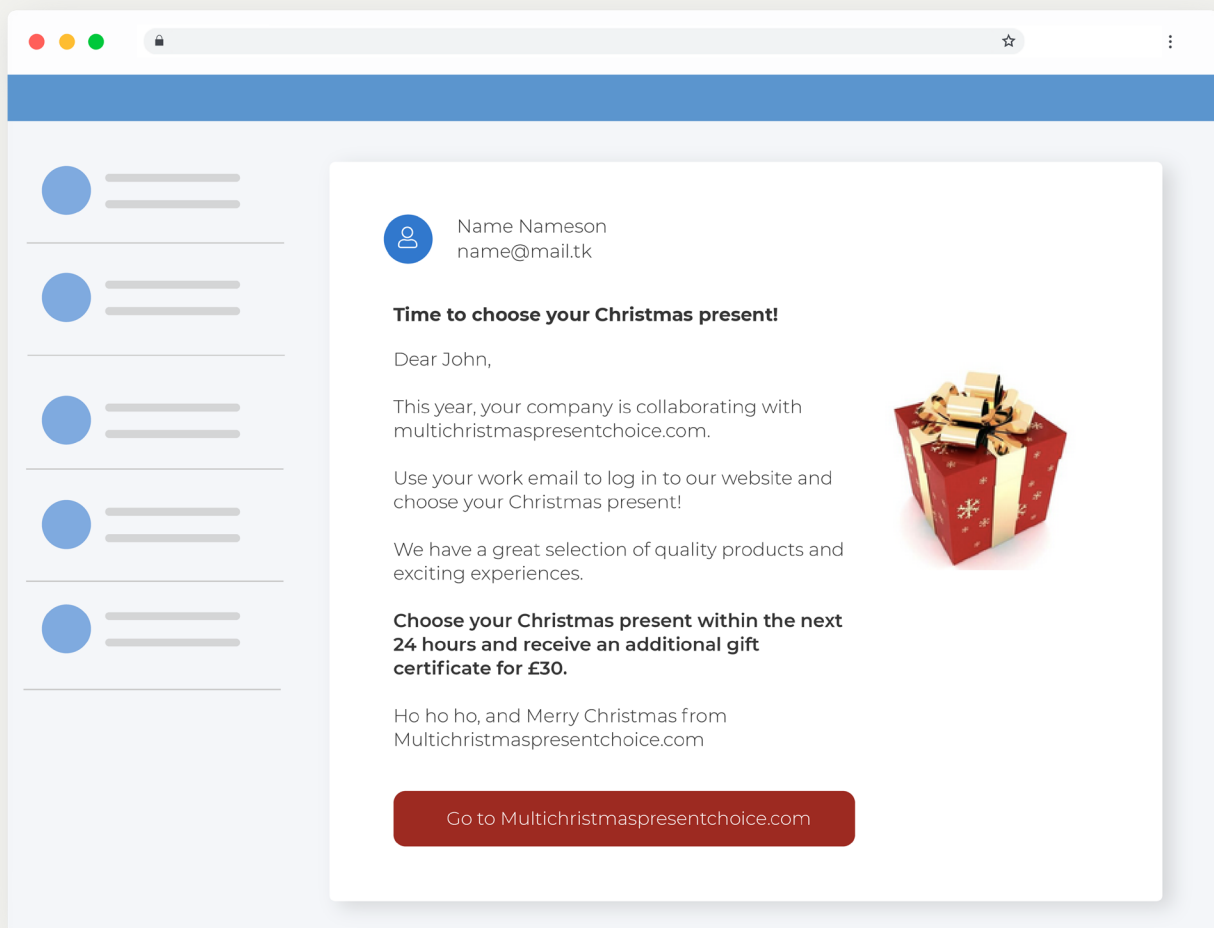


Phishing simulations - an example

Below, we present you with one example of phishing training. It shows you what a phishing attack typically looks like when it is targeted at an organisation. Cybercriminals try to be very personal in their approach and can be very persuasive for the receiver to interact with the phishing email.

Ideally, your team would simply counter the attack by ignoring it and deleting the email. However, they are also expected to bring this to the attention of their colleagues so they can avoid falling into the trap as well.

Example - The Christmas Present



**#4 Measuring is key
when you want to
secure long-term
information security
in your organisation**

| Tracking your progress

The top layer of the pyramid is an important part of the effort to improve your information security: **tracking your progress**.

Companies and organisations often implement a long line of measures but forget to assess if the efforts lead to the results they were looking for.

Without tracking your progress, it is impossible to know where you are and where you are headed. Not that we're saying that you should track every single parameter – but it is a good idea to set goals and milestones to know that you are making progress.

We recommend that you consider the following:

- What is the use of awareness training if your team doesn't adopt good digital habits?
- What is the use of attending the training if they don't understand the information?
- What difference does it make if your team has the appropriate information but cannot convert it into actionable steps?

We recommend that you measure the following parameters:

- Participation in the courses
- Results from quizzes and tests
- Phishing simulation results
- Changes in your team's digital behaviour
- Changes in the number of information security breaches

Statistics from real cases – information security is still a great challenge

Despite the increased attention to information security and the GDPR, there is no doubt that companies and organisations are still facing many challenges when it comes to information security.

At CyberPilot, we have conducted a few experiments that shed some light on this. The following numbers show just how relatively unprepared some companies are against phishing attacks.



Of the total number of sent emails, 56% of them were opened by staff, 27% clicked a link, and 17% gave out their email address and private passwords to unauthorised sources.

That is quite alarming, and these numbers underline the most important and fundamental point in this e-book:

Your employees are your greatest risk - not your IT.

This means you need to focus your effort on training your team to be aware of information security issues - that is the only way to establish a solid defence in your organisation and prevent potential attacks.

**Conclusion – achieve
your goal of
awareness**

The four steps to achieving awareness within your team

Regardless of how mature your company is when it comes to information security, information security and data handling will gain an increasingly large role in your work life.

That is because information security is here to stay, and it is an area where companies and organisations must work actively and continuously. If not, your workplace will be particularly vulnerable to security breaches which may ultimately lead to large fines and even loss of intellectual property.

Luckily, your company or organisation only needs to take a few simple measures to minimise this risk. In this guide, we have addressed the four steps that in our experience, create the best results.

Don't forget to get the free tools and different types of inspirational material to get you started (or go further) with your efforts to increase information security in your organisation. Just send us an e-mail at info@cyberpilot.io and we will be providing you with our templates and hopefully guide you in the right direction.

To summarise, it comes down to four steps:

- Clear communication
- Concrete guidelines
- Awareness
- Tracking your progress

Ideally, all the four steps would be implemented. If you succeed, you are well on your way to creating the change in company culture that is required to reduce the risk of human error when it comes to information security.

CyberPilot – your partner for information security and the GDPR

If you are looking for an impartial and trusted advisor to guide you and your team to strengthen the level of information security and GDPR compliance, then CyberPilot is here for you.

CyberPilot is a specialised information security company that helps companies and organisations of all sizes attain effective information security based on a firm belief in training teams in the safe handling of data in the workplace.

We have many years of experience in guiding and training organisations in information security and information GDPR. We specialise in:

- Awareness training (e-learning)
- Phishing training

We believe that information security isn't just a question of the technology, but just as much a question of people and processes, and this is evident in our services and solutions. We always start by improving human behaviour, awareness, and knowledge.

We offer courses and training that is adapted to your team's information security needs, challenges, and level of awareness. Our training and materials are developed to make complex topics as understandable and relatable as possible.

Contact us for a talk about what we can do for your organisation.

E-mail: info@cyberpilot.io

Telephone: +45 40 32 32 35

We look forward to hearing from you.