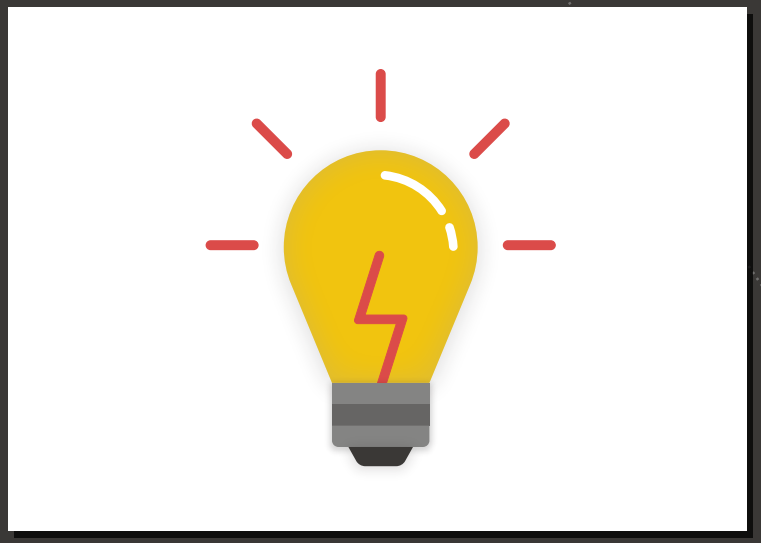
THE IMPORTANCE OF SECURITY AWARENESS TRAINING

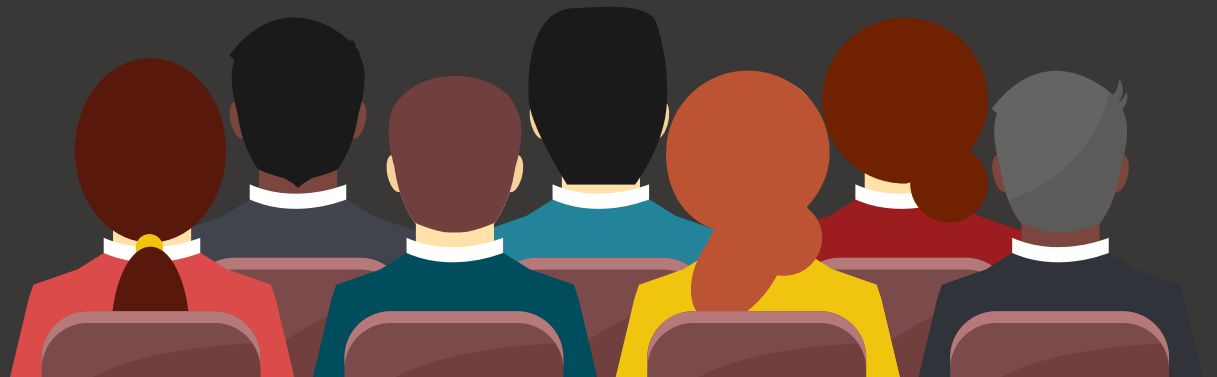
How to overcome the challenges of convincing leadership

inspired eLearning®
education for your enterprise

Security Awareness Training Programs

- Can be all encompassing or about specific security awareness topics
- Allow you to track the participation and success of your employees throughout the education process
- Come with blogs, newsletters, infographics, and more for ongoing reinforcement and refreshers throughout the year





inspired eLearning®
education for your enterprise

How do you show leadership that your organization needs security awareness training?

There are 5 key components to convincing leadership to invest:

Identifying the problem

Budget

Change Management

Lack of Understanding

Time Management

Clearly identify the problem you're trying to solve

What has caused the interest in a security awareness training program?

- ✕ Is it a phishing problem?
- ✕ Ongoing ransomware attacks?
- ✕ Tried a phishing tool, and your employees failed?

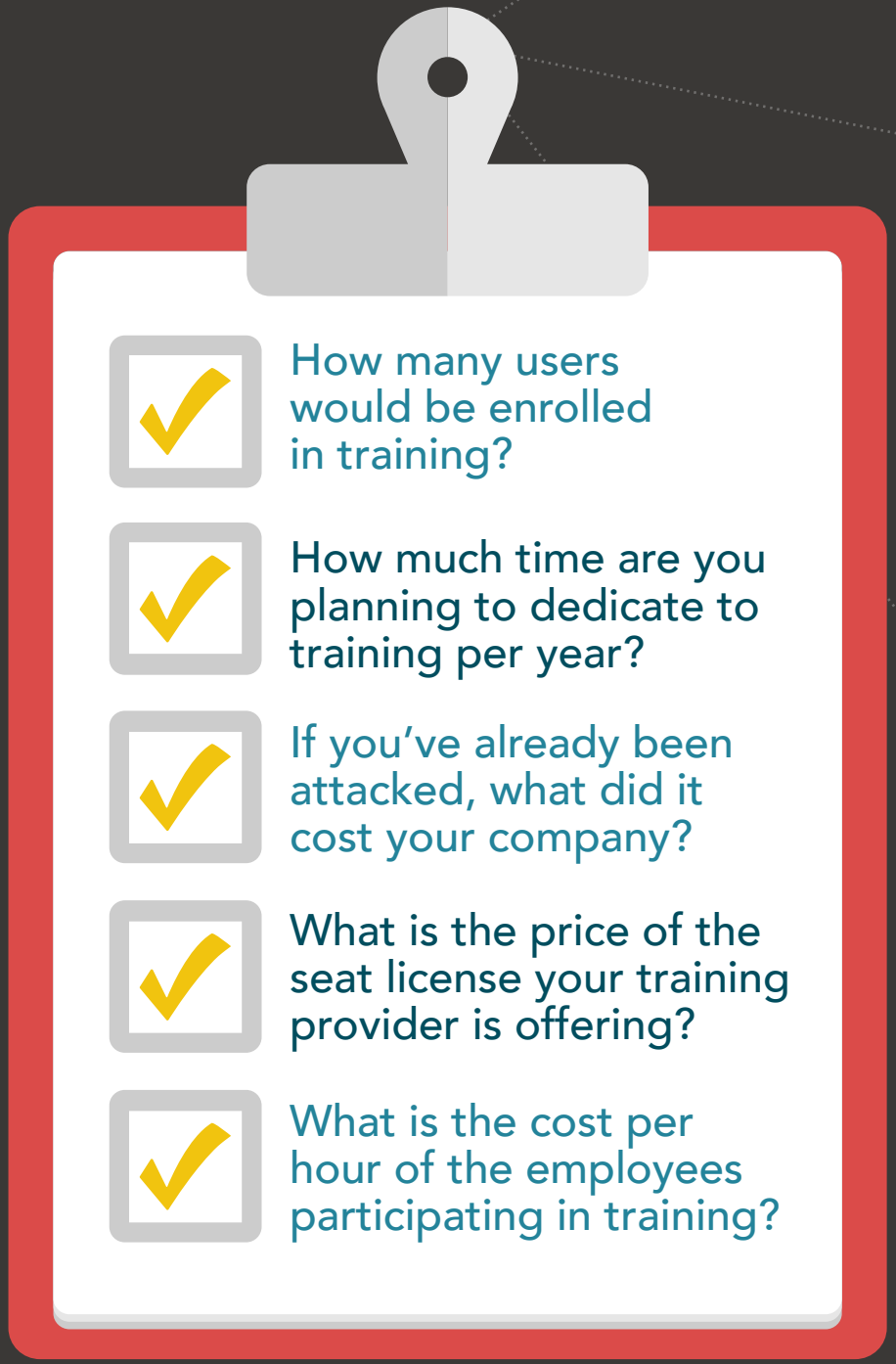
☛ Identify a specific example of how your organization's data was, or could be, compromised

Budget Challenges

Every leadership team needs to know the required spend and the potential ROI

On the next page, we'll show you a simple equation for calculating the ROI on security awareness training

Here's a checklist to prepare you for the equation:



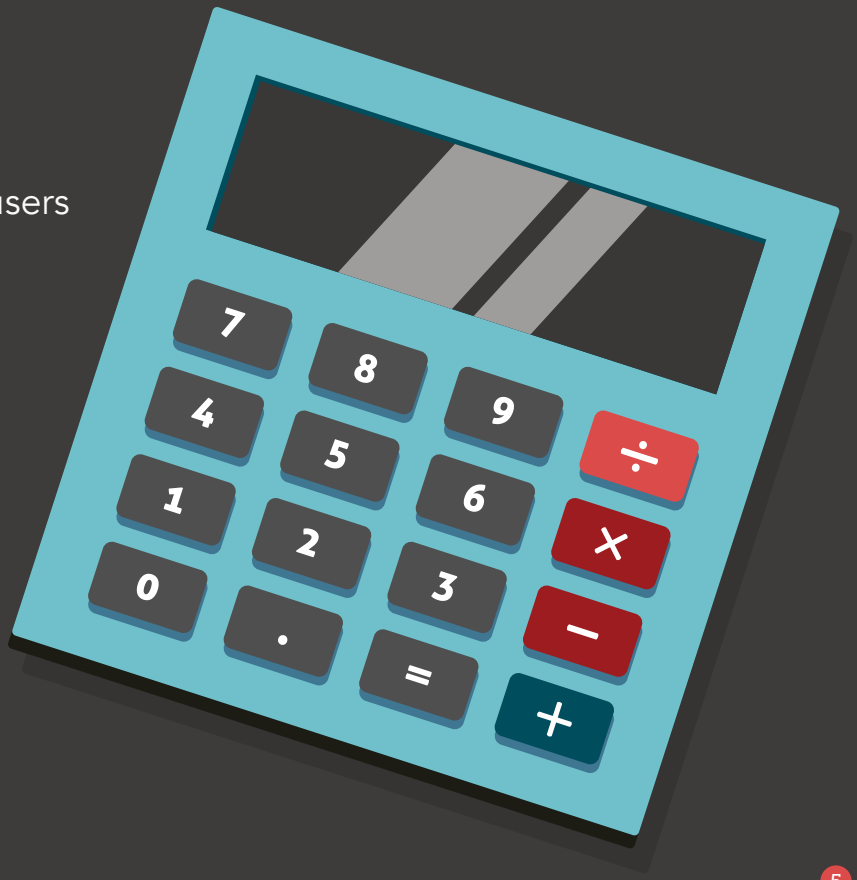
Calculating Security Awareness Training ROI

$$ROI\% = \left(\frac{savings}{cost} - 1 \right) \times 100\%$$

Savings = $100,000 - $150,000
The average cost of an attack to an SMB in the US 2017

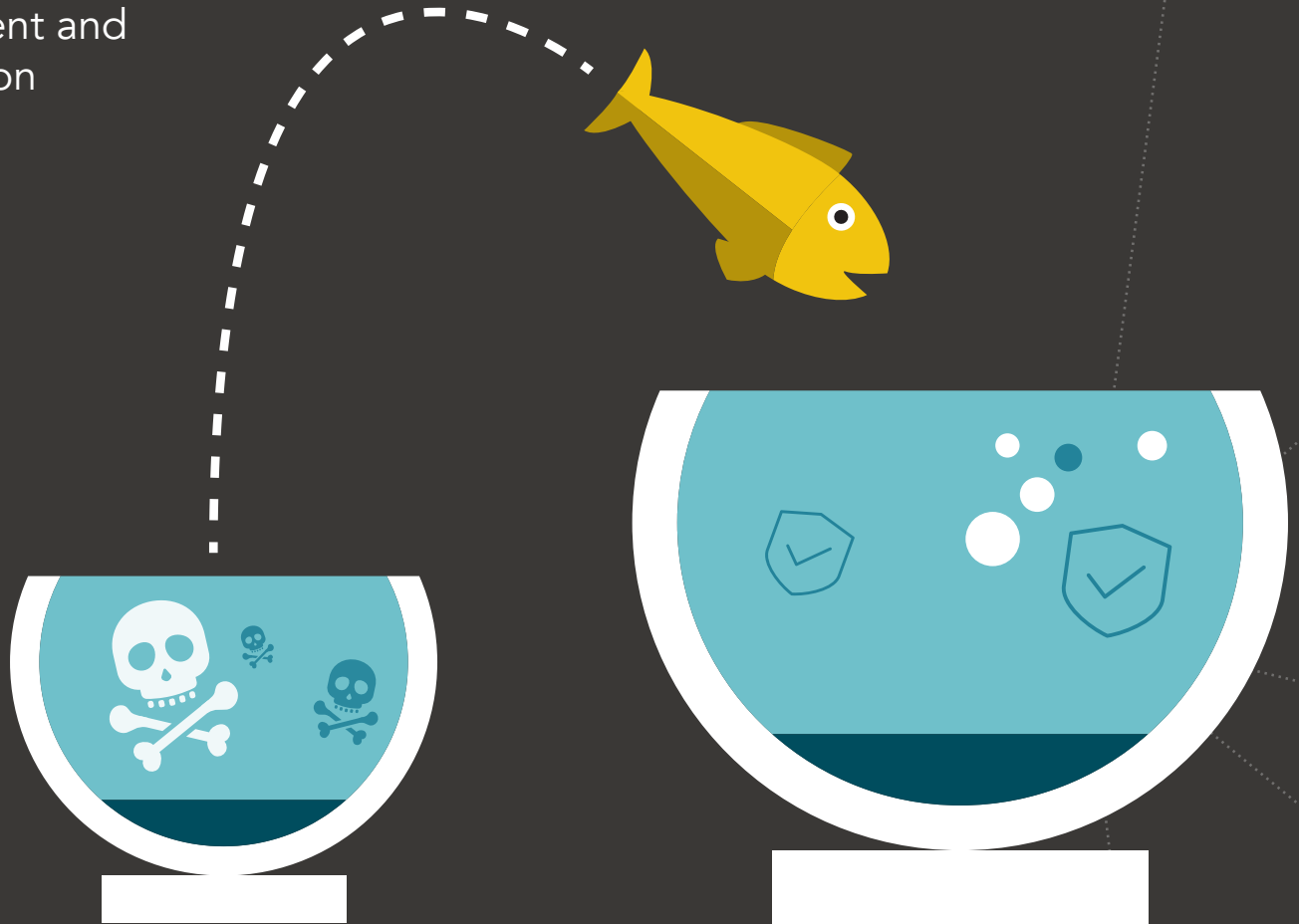
Cost = program + time allocation
Program cost = users X price per seat license
Time allocation = 4 hours per year X $25 per hour X number of users

Other key factors include:
Loss of revenue
Damaged brand reputation



Change Management

- People often resist change
- With leadership support, employees will understand the training is important and not optional
- Requires constant reinforcement and metrics to keep up participation



Lack of Understanding

It's often difficult for leadership to support a problem they don't fully understand.

Explain to leadership that hackers will look for the easiest way to get into your systems – your employees.

By providing security awareness training, your employees will be aware of threats and empowered to protect your organization.

You must shift the thinking from "cyber-security is ITs problem" to... "cyber-security is a company priority."

"Cyber-security is a company priority"

Cyber Attack Statistics

91%
of advanced cyber attacks begin with an email

97%
of people around the world cannot identify a sophisticated phishing email

In 2017, reports of W-2 phishing emails increased
870%

61%
of SMBs have experienced a cyber attack in the last 12 months

54%
of businesses site "negligent employee" as the root cause of data breaches

60%
of small businesses go out of business within 6 months of an attack

On average, it takes a company
206 days
to detect a data breach

On average, it takes a company
66 days
to contain a data breach

https://blog.barkly.com/phishing-statistics-2017
https://keepersecurity.com/2017-State-Cybersecurity-Small-Medium-Businesses-SMB.html
https://www.itgovernanceusa.com/blog/how-long-does-it-take-to-detect-a-cyber-attack/
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Time Requirements

- Time requirements can often be misunderstood
- A good training program is only 1-2 hours per quarter
- On average it takes 46 days to resolve a cyber attack

ATTACKS ARE HAPPENING NOW!

Don't wait until you're a victim of a cyber-crime to enroll your organization in a security awareness course.

Act now, and empower your employees with the tools needed to protect your organization.

inspired eLearning®
education for your enterprise

For more information contact us and we'll help you get your organization educated and protected.

800.631.2078

info@inspiredelearning.com

Online Chat:
inspiredelearning.com