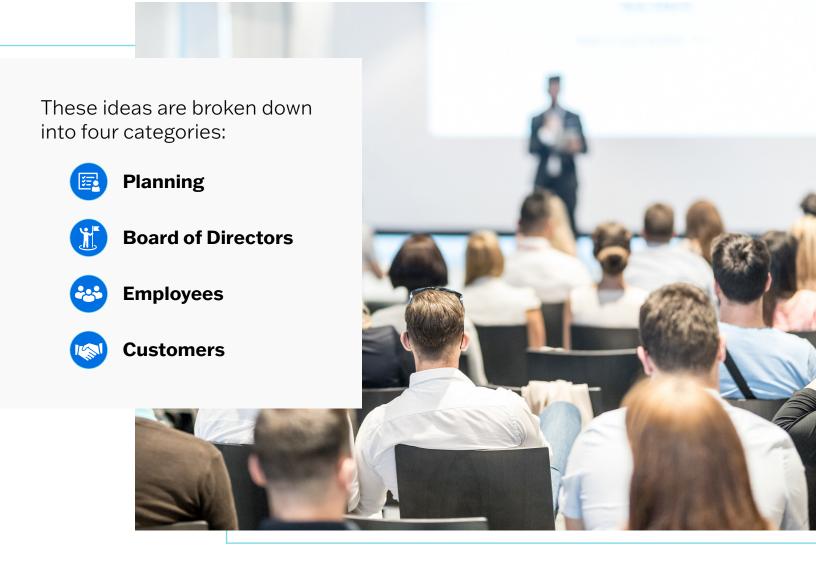![SBS CyberSecurity logo]

34 Unique Ideas to
Create a Culture of Cybersecurity

INTRODUCTION

The cornerstone of your cybersecurity culture is training. Implementing a consistent security awareness training program for your employees, board of directors, and even your customers helps establish trust that your organization takes cybersecurity seriously. Ongoing security awareness training throughout the year proves to be effective in reducing cyber risk for your organization, along with helping you stay compliant with laws and regulations. The following is a list of ideas to help promote a strong cybersecurity culture within your organization.

These ideas are broken down into four categories:

- **Planning**
- **Board of Directors**
- **Employees**
- **Customers**

PLANNING

1 Document Your Plan

Many companies conduct cybersecurity awareness training and host a variety of activities to increase security culture, but they don't have a documented plan to use as a guide. Build a plan that incorporates some of the considerations mentioned in this document, and use it as your map to success.

2 Get Buy In

Even if you are the cybersecurity awareness champion at your company, you cannot create a stronger security awareness culture alone. You will need to have full support from the Board of Directors, executives, management, and other key departments to get the greatest result. Use the latest security breaches and news stories to help gain buy in from your team.

3 Make It Personal

Those who are close to cybersecurity understand the importance of cybersecurity at work and at home. However, many people only think about it when something big happens. Start with programs to help employees protect their personal information and they will tend to be more attentive and engaged in understanding cybersecurity at work.

4 Use a Layered Approach

We hear the **layered approach** terminology all the time in the cybersecurity world. This term also applies when building an awareness program. Everyone in your organization has a different learning style and if you are deploying one approach to awareness you will have ineffective results. Plan to use multiple ideas and approaches to increase the effectiveness of your program.

5 Measure Success

Ok, you have created your cybersecurity awareness program and have deployed an array of approaches to raise awareness. How do you know that it is working? What approach seems to be working more than others? How do you measure that? Some measurements are easier to gather than others; however you can establish a baseline through quizzes, phishing failures, engagement levels, course completions, and even attitude checks.

BOARD OF DIRECTORS

6

Create a Standing Agenda Item

Incorporate 5-10 minutes at **every** board of directors meeting to educate about cybersecurity or discuss recent threats and how they could impact the company. Make sure to document these activities in the minutes.

7

Get the Board of Directors Involved

It is always beneficial for company moral to see owners and leaders of the company at scheduled trainings and events. Their attendance and support shows that they have bought into the idea of a stronger cybersecurity culture and see it as an important cause.

8

Go Phishing

Don't let your board off the hook! Treat them like everyone else when executing a phishing assessment.

9

Bring in an Expert

Having a cybersecurity expert discuss the trends that they are witnessing in the field and risks associated can generate increased buy in from the members of the board.

10

Get Certified

Send the members of the board through a cybersecurity certification program or have them attend an event that focuses on how to manage cybersecurity at the board level. The SBS Institute offers the Certified Banking Security Executive certification tailored to provide a clear understanding of management requirements for cybersecurity and a strategic technology background for future planning.

EMPLOYEES

11 **Invest in Tools**

Investing in automated cybersecurity awareness and phishing tools, such as KnowBe4, can create a repeatable model to deliver education. These tools can be a cost-effective way to enhance your cybersecurity awareness culture.

12 **Gamify**

Incorporating game-like elements into training material is an effective technique used to engage learners. Automated tools have great interactive games built into them to challenge your employees. If you do not have the resources to invest in software, create your own crossword puzzle, Jeopardy or Family Feud game.

13 **Follow the Experts**

Find cybersecurity awareness companies and follow them on social media. Many of these companies offer creative videos and documents that you can incorporate into your program.

14 **Engage in One-On-Ones**

Most companies conduct their training in groups. However, some of your employees might not feel confident enough to ask questions or speak up in a group setting. If you have employees like this, you may get better results with individual training.

15 **Create a Rule**

Create a rule to flag any email from external sources as an "External Email." This should alert the employee to think twice before they click.

16 **Bring in an Expert**

Hiring an external resource to present to employees can increase engagement. Many speakers will also make it fun by incorporating games or having rewards for participation.

EMPLOYEES

17 **Share Posters and Articles**

Place posters, articles, or other educational materials in the break room or other meeting areas.

18 **Conduct a Test**

An excellent way to test your employees' level of awareness is to conduct social engineering assessments. These can be executed internally, or you can hire an external firm to complete the assessment.

19 **Share Monthly Tips**

Send out a monthly cybersecurity newsletter or tip to all employees to keep them engaged.

20 **Set Computer Backgrounds**

Push out cybersecurity tips and posters as the background to all employee computers. A selection of tip graphics and posters can be downloaded at: sbscyber.com

21 **Allow the Student to Become the Teacher**

Encourage your employees to create a presentation based on a cybersecurity topic. They can share their presentation internally or with the community as a service opportunity.

22 **Reward Good Behavior**

Implement a rewards or recognition program to show appreciation for following through with training, applying concepts, or passing a social engineering test.

23 **Send Security Alerts**

Get in the habit of sending out cybersecurity alerts to all employees when there are known threats that affect the company.

CUSTOMERS

24 **Make it Fun**

Share quizzes, crossword puzzles, or games to get your customers to start thinking about cybersecurity topics. Provide a prize or drawing for those who participate.

25 **Focus on Personal Security**

Your customers, much like your employees, will pay particularly close attention when discussing cybersecurity topics relating to their personal lives. Focus education efforts on how they can improve personal security with subjects such as safe web browsing, mobile phone usage, trustworthy wireless connections, and how to spot a phishing email.

26 **Utilize Your Company Website**

Place or link to relevant cybersecurity tips, news stories, and alerts on your website.

27 **Take Advantage of Hold Music**

Incorporate cybersecurity tips into your on hold message when customers call your business.

28 **Host a Security Awareness Day**

Host a cybersecurity awareness day where customers can come to your office to shred sensitive documents, play security-themed games or trivia, and enjoy the community.

29 **Present a Lunch and Learn**

Plan a lunch and learn event that focuses on the latest cybersecurity trends and tips for securing their business.

30 **Send Security Alerts**

Get in the habit of sending out cybersecurity alerts to customers when there are threats to their personal security.

CUSTOMERS

31 Share Monthly Tips

Include a tip in your monthly newsletter to keep cybersecurity top-of-mind for your customers.

32 Become the Expert

Consider writing whitepapers or blog posts and conducting radio or newspaper interviews to build brand and cybersecurity awareness.

33 Follow the Experts

Encourage your customers to follow your organization on social media as you create and share cybersecurity tips and news.

34 Share Posters and Articles

Place posters, articles, or other educational materials in the lobby, entrance, or other customer accessible areas.

Free Resources

available at: sbscyber.com

Hacker Hour Webinar
Join our free monthly interactive webinar series focused on discussing cybersecurity issues and trends.

Product Demos
Discover the power of our offerings with live demos scheduled each week highlighting individual products and services.

Security Awareness Training
Share our cybersecurity training tools with both your employees and your customers.

TRAC™ Action Tracking
Remain diligent with your remediation tracking and follow up by creating security plans associated with your risk assessment.

Join Our Email List
Follow the latest trends in cybersecurity, information technology, and upcoming educational events from SBS CyberSecurity.

Your Cybersecurity Ally

SBS CyberSecurity, LLC (SBS) is a top-rated consulting and audit firm. With over 20 years in the cybersecurity industry, SBS has provided solutions to thousands of regulated organizations across the United States and abroad. We offer dynamic solutions to help you build a proactive risk management program capable of withstanding the daily threats your organization faces. Our services are designed to assist you in making informed cybersecurity decisions to better protect your business.

For more information:
sbscyber.com | 605.923.8722