PRINCIPLES OF...

BUILDING A STRONG CYBERSECURITY CULTURE

SECURITY PURSUIT

CULTURE

Company culture is more important than ever. With low unemployment and the Great Resignation in full-swing, having a positive and productive company culture is proving to be a "must-have" rather than a "nice-to-have."

Building a great company culture is important not only for employee engagement, happiness and retention, but it also drives the organization's ability to effectively meet its mission.

At the same time, ransomware, vendor compromise, BEC and countless other threats makes it more important than ever to have a strong **security culture**. Employees are your first line of defense. Phishing tests and security training help, but employees still fall prey to innovative attacks.

Organization culture and security culture are not independent. They need to be deeply connected in order for security to be considered an integral part of the organizations mission and values.

How can you create a culture that embeds security into everyone's daily work while making the security team a partner? This white paper describes what is required. It is based on the principles we follow with our...

Security Culture Program. Let's get started!

What is a Security Culture?

Every organization has a culture, whether by design or not. Culture is a collection of values, behaviors, working practices, and beliefs that employees share while aiming to fulfill the organization's collective purpose. It is a reflection of all the ways employees interact and what you collectively value.

Your security culture must be an extension of this, and it must integrate into the existing operational culture to embed security into employee's daily work life. Culture is what drives behavioral change, and security culture is no different. Security culture means people recognize their role in protecting the organization's assets.They take ownership and see themselves as a key player in your overall security program.

What are the Benefits of a Security Culture?

Security culture is important, whether you're an organization of five people or five thousand. With a strong security culture, individuals will operate safely, be mindful of ongoing risks, and make better decisions. The benefits will be felt at every level.

Here are just a few benefits of a strong security culture:

- Fewer compromises, of course.
- Compromises that do happen are identified more quickly, allowing for faster response, creating less impact.
- You and your security team are viewed as enablers...not "no-sayers" who put up roadblocks everywhere.
- You share the burden of compromise...it's not all your fault.
- Budget requests become easier when security is everyone's concern.
- Vendors become more aware of your expectations as they work with line-of-business leadership.
- You have personal and professional growth beyond technical concerns, increasing your value.

What does Security Culture Look Like?

Great Culture	Terrible Culture
"I do Accounts Payable and I know hackers may try to setup a fake vendor."	"I do Accounts Payable. Why would someone attack me?"
"This looks suspicious. I'm going to Slack our security team."	"Huh. It looks like this vendor wants their bank account changed."
"Oh no...I don't think I should've clicked on that. I need to Slack our security team.:	"Oh no...I don't think I should've clicked on that. I hope no one notices."
"Mike, you shouldn't be putting customer records in that unapproved cloud app."	"That's a cool app, Mike. Just don't tell the security team 'cuz they'll cut you off!"
"I just told my husband that we need to have longer passwords on our personal Amazon account. 16 characters!"	" I just use "cutiepie" for my password on all my personal stuff."
"I can't wait for our security training this afternoon. I have so many questions."	"I'll work on that report this afternoon during that security thing."
"Great...MFA was approved in the budget!"	"How many more barriers to work do we need around here?"

6 Elements to a Security Culture

Building a Security Culture takes time and planning. Our Security Culture Program follows six elements that are key to security culture building.

Use these as you build and execute your program.

1. Current State Alignment

Start with an honest understanding of your organization's current security culture. This goes well beyond the results of your last phishing test. It requires talking to people and getting their live feedback. For smaller organizations, it can be quickly accomplished with several short meetings with various staff. For larger organizations, we do this with a survey to a representative sample of employees, followed by select interviews.

When interviewing employees, you need to understand the real level of their awareness from a cultural standpoint. You want to question employees on:

- Their understanding of how cybersecurity aligns with the organization's goals.
- What cyber risks the organization faces in accomplishing the strategy.
- What data and assets are critical to the organization and need to be protected.
- The unique risks associated with their department and individual role.
- Awareness of:
  - Security principles
  - What is expected of them through documented policies
  - Incident identification and response.

You may have much of this information already, but it's good to establish a formal baseline to measure progress against. While doing the interviews, be sure to identify advocates in each department. You will need them.

OnDev Apps aims to create an app to cover these industries. We will partner with different institutions that have a need for an app.

2. Social Engineering

Many organizations look at commercial phishing tools and believe that's enough to build awareness. They definitely help with awareness, but they won't help you build a security culture. In fact, we've seen them really hurt culture.

We run a variety of tools for clients from KnowBe4, Phishme, Mimecast, ProofPoint, etc. Some tool vendors recommend running phishing as often as every two weeks. They also recommend making people that fail be required to take one of their online courses. For most organizations, this will effectively kill your security culture. Plus, people will hate the security team.

Don't get us wrong...we like the tools and recommend them for many clients. Just keep in mind a) you may not need or want a tool, b) they can hurt culture if used wrong, and c) they are just a component to your security culture.

You may be better off doing highly customized social engineering campaigns that align to the unique nature of the organization, the department you want to test, and even the individual. Tools have hundreds or thousands of scenarios to choose from, but they are often just a bit "off", making them easier to identify as a test. Highly developed phishing campaigns done outside of tools provides a much better perspective and usually elevates awareness beyond a tools-only approach.

It's also important to build other methods of social engineering into your program beyond just phishing. Other forms of social engineering broaden the exposure to your employees. Some that have proven highly educational include:

Physical Exploits

Pre-Text Phone Calls

Social Media Attacks

Smishing

LinkedIn Phishing

Vishing

3. Training

Phishing tools, antivirus vendors and others have online training courses. Some are good... some are horrible. Seeing one cartoon character coach another on basic security is almost always ineffective and frequently insulting. Like Phishing tools, online courses can kill your security culture.

The implementation of online courses is often wrong. Although you may need to for compliance purposes, making courses mandatory hurts culture without all the other elements listed here. In addition, training should rarely be used as a punishment or stick because a person fell prey to a test or event.

Custom online courses tuned to your business are highly effective. They don't have to be overly expensive and usually have a 12-month shelf life. Using online tools is convenient and easy to measure, too. We like to create and use them for foundational courses for new employees and core concepts.

A central component to building a security minded culture is live training. There is nothing like having an expert create and deliver custom training programs to your employees. Use live training to build on core concepts (perhaps from online courses) and tune it to your unique situation. Live training also lets you talk about the latest cybersecurity issues in the news. Did something happen this week, either in the organization or in the news? Talk about it!

We recommend talking about cybersecurity at home, too, to make it even more personal. You want your employees to live a safe digital life at work and at home.

Of course, Live Training provides time for open Q&A. This puts employees into the conversation and leaves no questions unanswered.

4. Department Coaching

Building a culture is all about knowing your role in the organization's mission. You want individuals to "own" their job and take pride in it. The same applies to cybersecurity. Department coaching is where security culture magic happens. It allows employees and their closest co-workers to align on their mission and the risks that threaten them.

These should be intimate coaching sessions with leaders and employees to review more specific risk scenarios for those teams. Doing it over lunch, perhaps with pizza or sandwiches, removes pressure and creates a fun open atmosphere. We are always amazed at the insight people have, which can play a further role in your broader cybersecurity issues.

5.Fun & Games

Quick reminders keep cybersecurity top-of-mind and in the flow of work. A poster here, an infographic casually shared, occasional intranet banners and periodic newsletter content. Variety and consistency counts. We recommend simple and quick. Such reminders should be non-intrusive but on-point with the security culture you are building.

Cybersecurity is serious business, but that doesn't mean you can't have a little fun. We're talking culture, after all. Rewarding employees for catching phishing is a great start. How about a contest for writing the best home-grown phishing email so employees can think like a hacker! Have leaderboards, award certificates and more. Adding in a bit of fun and competitiveness can make all the difference to your security culture.

6. Measurement

Remember…measurement is easy in cybersecurity. Making measurements meaningful is very hard. But it is imperative to do so if you want to continue to fund your security projects. Can you measure culture?

We believe you can, but it needs to be logical if it is to be believed. There are three layers in which to measure the progress of your security culture:

Measure AWARENESS with TESTING

Simulations are next, and they are not tests. We like to see awareness being tested thru actual online tests, given periodically to employees. Are employees aware of policy requirements? Do they know who to call when they see a threat or suspect a compromise? Do they know what assets and data are most sensitive in the organization? Testing gives you measurable information that you can't get elsewhere.

Measure BEHAVIOR with SIMULATIONS

Phishing, social engineering, tabletop testing and participating in events go beyond knowledge to the realm of measuring behavior. Exposing people to realistic cybersecurity simulations in the heat of their day is where you measure behavior. How many and who shows up to training reflects individual's commitment to security and their job.

Measure CULTURE with SURVEYS

Creating the culture you want can be elusive. The best way to measure it is with surveying. Ideally, you should tie your security culture survey into larger organizational and/or department surveys. Use open ended questions with narrative responses to allow employees to explain their thoughts in their own words. "Why does our organization exist? What is your role? How does cybersecurity help us achieve our goals? Etc." Be careful of labeling your culture as "good" or "bad". Instead, look for consistency in responses. If you don't see consistency, tune your program.

Use each of these to conduct further measurements so you know where to tune your program. If people are doing great on phishing, but fail on physical attacks, then you know where to invest a bit more time.

Putting It All Together

The current business climate leaves no room for companies with bad culture. Labor markets are tight, and employees have many options on where to work. Your CEO, HR executives and department leaders are struggling to attract and keep the best employees. Checking the box by simply doing phishing tests and basic training will not be enough today.

Instead, use the ideas in this white paper. Align cybersecurity to the bigger purpose of the organization. Use what your company says publicly. Talk to your HR executives, department leaders, and executive management. Build and integrate your cybersecurity culture into the hearts and minds of every employee.

Next Steps

Want help building a cybersecurity culture? Security Pursuit has given a lot of thought to helping clients build a cybersecurity culture. Culture is imperative if you want employees to take ownership in your security program; if you want your budget needs to be inherently understood; if you want to be part of key strategic decisions of the company; and, if you want cybersecurity to be seen as an enabler to innovation.

We call it, “Security Culture Program". Working with you, we build, manage and report on your security culture program.

Contact us today to learn about our Security Culture Program

SECURITY PURSUIT

720-675-ROOT (7668)
www.securitypursuit.com