Why an organization’s security starts with its culture

The better it changes, the better you can. The need to secure your organization’s digital infrastructure has never been more vital. And with this need comes an opportunity to evolve the ways in which you secure your organization – one that will become a center of a cultural shift – one that will become a powerful defense against digital threats.

Security is a part of your culture

If your organization is encountering low levels of employee participation in security, it might be the result of your workforce’s belief that it is not everyone’s responsibility. It certainly is everyone’s responsibility. Your employees are your strongest defense. If they aren’t engaged, your security risk is significantly increased.

As the story you wish to tell is influential to all employees, it is the way you design your organization. You can’t create a secure culture by standing an organization on its head. One that promotes secure behavior is the one that is designed to do so.

Your people are ready

It’s not about training employees. It’s about designing a culture where employees want to do the right thing. It is about creating an environment where employees can make ethical decisions in the moment.

Employees who believe that most cyber security issues are their responsibility are more likely to engage in security practices, and are more likely to report threats. When employees are engaged, they are more likely to look for security gaps that will only grow wider.

The desire to change pulls one way. The need to stay in place pulls another. And as organizations have embraced new ways of working, they have needed new security protocols that only grow more vital.

We need a security culture. Smart Culture.

To build a stronger security posture, it’s going to take everyone and everything – people, processes, and technologies – working together to secure the whole business. That’s a security culture and it’s one that you can help build.

After all, it’s their organization, too.

So, that more creative and interactive approach is an effective means to encourage the right behavior and to engender a sense of responsibility. And it’s the foundation that is helping security practices evolve into the 21st century.

Employees who believe that most cyber security issues are their responsibility are more likely to engage in security practices, and are more likely to report threats. When employees are engaged, they are more likely to look for security gaps that will only grow wider.

The desire to change pulls one way. The need to stay in place pulls another. And as organizations have embraced new ways of working, they have needed new security protocols that only grow more vital.

We need a security culture. Smart Culture.

To build a stronger security posture, it’s going to take everyone and everything – people, processes, and technologies – working together to secure the whole business. That’s a security culture and it’s one that you can help build.

After all, it’s their organization, too.

So, that more creative and interactive approach is an effective means to encourage the right behavior and to engender a sense of responsibility. And it’s the foundation that is helping security practices evolve into the 21st century.