WIMsecurity

WHITEPAPER #1

Security Culture As a Strategy

Jovica Ilic

wimsecurity.com

Improving Security With Little to No Financial Investment

EXECUTIVE SUMMARY

If implemented correctly, Information Security can be a business enabler. You can avoid the majority of security risks to your business by making security a daily consideration in your organization. The best way to do this is through a good security culture.

It's a common myth, that people resist change. People resist change only when it comes with ambiguity. If you remove the ambiguity, people won't resist the change.

There are two crucial rules to success in any organizational change. First, perception is reality. Second, people don't believe in what they read or hear, they believe in what they see.

To change the culture, you need to change people's behavior. To do that, you need to change their belief systems. The only way to do this successfully, is to start at the top.

YOU, TODAY

The Information Security domain is usually perceived as a cost center in many organizations. We've proven it to many clients that it can actually be a business enabler, if done right. Have a look at our ISO27001 Case Study on our website.

In the times of financial crisis, reducing costs becomes a priority. On the other hand, the cyber threats are constantly evolving, and your business has never been in a bigger danger from cyberattacks than it is today.

You are a target, no matter what you think. A cyber attack on you is not a matter of IF, but WHEN. And no, I'm not trying to use FUD (Fear, Uncertainty and Doubt) as a tactic here. I actually loathe it.

All I'm stating here are just the facts. I could give you some statistics, but most cybersecurity stats are useless. That's another topic covered in my book on Information Security strategy.

SECURITY CULTURE AS STRATEGY

So the question is, how can you drastically improve the security of your organization, with minimal costs?

Depending on your organization type, size and the industry you're in, the answers can vary. There could be more than one best strategy. However, for any organization, one strategy will always be on the list. And that's building Security Culture.

Our experience shows that the organizations with the most security issues are those where the work is performed in this way:

- Step 1: Get some work done without thinking of security.
- Step 2: Get hacked.
- Step 3: Discover what in Step 1 introduced a vulnerability that allowed Step 2 to happen.
- Step 4: Secure the organization against the specific attack in Step 2.
- Step 5: Move on. Get some other work done.
- Step 6: Get hacked again.
- Step 7: Find out that, during Step 5, another new vulnerability was exploited, relating to work in Step 1.
- Step 8: Repeat Step 4.

You can avoid the majority of security issues and risks by making security a daily consideration of your every employee. This is why you need to build a security culture in your organization.

The way we build a security culture, gets our clients to work more like:

» Step 1: Think about the security of proposed work and make it part of your decision-making.

» Step 2: Get some work done, while still taking security into consideration.

Step 3: Continue to think about security.

» Step 4: Repeat Step 1.

This sounds easier than it actually is. There are many factors which add to the complexity of such a solution. I'll mention only one.

Security culture can be, in simplified terms, described as what your employees do when faced with situations for which there are no rules or policies defined. Those are the situations when they need to apply their own judgment to make decisions on which actions to take.

Such situations happen frequently. No matter how great your security policies are, it's impossible to come up with rules for everything. Instead of hoping for their good judgment, you can provide your people with a tool which they can use in such situations.

This tool could be a short document with a well explained process for decision-making. A well-defined process will keep the judgment of your employees within your desired framework. Additionally, it would reduce the impact of their biases. Reduce, not eliminate. But, it's a good start.

THE CHALLENGE OF CHANGE

Creating or improving your organizational culture means change. The same goes for security culture. You should look at it as a subset of your organizational culture.

We all know that people resist change. Hence, that makes changes difficult to implement. However, that's not really the case.

Our experience, as well as the latest research in human psychology, suggests that people resist change only when it comes with ambiguity. If you remove the ambiguity, people won't resist the change. This is a big thing! It's one of the key principles to keep in mind when you're trying to drive an organizational change.

If we define culture as a set of beliefs that govern behavior, we can define security culture as a set of beliefs that govern security-aware behavior.

To support the new strategy of building a security culture, we often have to change or update organizational values. But, changing values is rarely a good place to start.

In general, it's easiest to change the behavior of your people. People's behavior is very susceptible to rewards, punishments, and external influences. This is the key.

WHERE DO YOU START?

There are two unwritten rules which guide behavior in any organization. They are straightforward. This is what WIM Security provides after all, simple yet effective solutions.

Our experience shows that many business leaders we meet are not really, consciously, aware of these rules:

- Rule 1: Perception is reality.
- Rule 2: People don't believe in what they read of hear, they believe what they see.

Being aware of these principles is crucial to the success of any initiative to change organizational culture. Still, awareness is not sufficient. So many doctors are aware that smoking is horrible for their health, yet they still smoke.

So here's the secret for WHAT you need to do. When it comes to HOW, we use our proprietary framework which is not covered in this whitepaper.

To change the culture, you need to change people's behavior. To do that, you need to change their belief systems. The only way to do this successfully, is to start at the top.

People look up to their managers. Managers look up to senior executives. Only once the senior executives change their behavior, belief systems of their subordinates, managers, will change.

Once managers update their belief systems, their behavior will change too. Moreover, when that happens, everyone reporting to those managers will update their own belief systems, and follow their manager's behavior.

This is the only way to build a security culture and have all your employees committed to keeping your organization secure.

This would drastically improve the security of your organization. You'd need to invest very little financially, if at all. But you, as an CEO or executive in charge, would need to invest your time and effort. With our help, this is actually quite effortless for you.

Sounds interesting? Contact us at hello@wimsecurity.com and let's have a chat.

Whitepaper #1
Security Culture As a Strategy
Improving Security With Little to No Financial Investment

Published by WIM Security GmbH.

Feel free to ask for permission, because you never know what our answer might be.

The information in this document is accurate to the best of our knowledge at the time of writing. As a reader you need to accept full responsibility for your actions and should consult with a professional about your own circumstances before following anything in the publication. Results are not guaranteed, just as nothing in life is guaranteed either.

Further, the author and publisher have used their best efforts to proof and confirm the content of the files, but you should proof and confirm information such as dates, measurements, and any other content for yourself. The author and publisher make no warranties of any kind, express or implied, with regard to that content or its accuracy.

For more information, please write to:

WIM Security GmbH
Pappelallee 78/79, 10437 Berlin, Germany
E-mail: hello@wimsecurity.com
Website: www.wimsecurity.com
Published in Berlin. Version 0.1.