ITsMine™

# IMAGINE PROTECTING HALF YOUR ORGANIZATION

**Imagine protecting only half of your organization. Pretty pointless, right? Well, that's what many organizations are doing when they focus exclusively on the threat posed by external attackers, while ignoring the threat – both malicious and unintentional – emanating from within the organization.**

ITsMine CEO Kfir Kimhi got together with Yaron Levi, CISO for Blue Cross and Blue Shield of Kansas City, to discuss this major threat – and how organizations can and should be dealing with it.

Yaron is the CISO for Blue Cross and Blue Shield of Kansas City (Blue KC). Before joining Blue KC, Yaron was a Director of Information Security for Cerner Corporation; an Information Security Business Partner for Intuit; an Information Security Architect and Product Manager for eBay; and a Director of Cloud Security for ANX. Yaron is a Research Fellow for the Cloud Security Alliance, serves as an advisory board member for several information security companies, and is the co-founder of the Kansas City CISO forum and B-Sides Kansas City.

In the conversation, Yaron brings his tremendous experience and knowledge to bear on this crucial subject.

**Kfir:**

Let me start by setting the scene. Company X has solutions in place to protect against external attackers. The tools they use are powerful – but only effective against attacks coming from outside of the organization. We say they are completely exposed because they've only solved half the problem.

**Yaron:**

What do they have in place to protect against the threat that is posed by people within the organization? Usually these are non-malicious – an employee that makes an error or a misjudgment resulting in compromised data. Moreover there is always the risk of a disgruntled employee accessing data and passing this on to unauthorized parties.

For example, many people view their work product as their own. Let's say a presentation they created or a complex spreadsheet or model. When they leave their job, they want to take it with them. In 99% of the cases they are doing this just to make their lives easier in future jobs, but from their employer's perspective this may be serious theft of intellectual property or even a violation of a regulation or law.

There are also cases where an attacker has compromised an employee account and is now acting as the employee. For all intents and purposes, this is another form of an insider threat.

**Kfir:**

I'd like to shift our focus to what organizations can do to protect against the insider threat. If we look at the world of email phishing for example, the most effective approach has been shown to be a combination of sophisticated technologies and employee training and awareness, with companies like Knowbe4. We maintain that this approach is needed when it comes to data security – which is a lot bigger than phishing.

**Yaron:**

This type of approach is critical. This has always been a tricky situation from people, process and technology perspectives.

**Kfir:**

So we know that when it comes to data protection, the insider threat is immense, and that many organizations aren't protected against this threat. And we know that the most effective approach is one that combines technological preventative measures with education for employees and reinforcing the right behaviors. What about KPIs? With the email phishing example we discussed, you can see how many people clicked a phishing email, you can get full analytics, and you can set goals and measure your success. With traditional DLP tools, it's a never-ending stream. Are there effective KPIs for insider threat?

**Yaron:**

That's exactly right. KPIs are a challenge that many security teams struggle with. It is not that we don't have metrics, we do, but most of them measure the noise level and are not actionable. It will be extremely helpful to have data centric and user centric KPIs that will allow the organization to better understand how big is the problem and what actions will need to be taken in order to reduce the risk.

I think there is another perspective to consider. We often speak about the CISO wearing many hats, but in this context, I want to refer to two hats in particular. These hats are the soldier, and the police officer.

**The first hat we wear is the soldier.**

Protecting our organization from external threats and penetration by the enemy. Here we can use powerful weaponry to achieve our goals. But if we try to use these weapons internally, it would be too much. Employees wouldn't be able get their work done, and it would be just as bad as having no protection at all.

**The second hat is that of the police officer.**

Making sure that people within the organization obey the law. This includes explaining why things should be done a certain way, educating and warning employees, and ensuring rules are actually kept for the safety of everyone. In a worst-case scenario, this also includes dealing with a "terror attack" inside the city – a malicious actor that has gained access to our system.

A great example of the police officer approach is with traffic violations. In many countries, if you collect too many traffic fines, you have to complete a course in order to start driving again. The course reinforces "healthy" and safe behaviors. This is a big part of the policeman role.

This is an important distinction. Being a soldier is easier in the sense that you know you are fighting an external enemy so in your mind it makes it pretty clear cut. On the other hand, as a police officer you are not dealing with "criminals", so to speak, all the time. And even when you do come across these "criminals", they may be your fellow citizens or co-workers which makes it much more difficult technically and mentally to deal with.

I think that most security people don't like to be the police and to keep switching between these two personalities. Moving constantly between soldier and police officer is really difficult.

**Kfir:**
That's right. Continuing with the police officer paradigm, this is something that's really at the heart of what ITsMine offers. For example, our software mines are used to see if employees access files they shouldn't. Planted throughout the organization, this feature alerts administrators to improper file use, but also reinforces the correct behaviors for employees. And employees know and feel that ITsMine is always there, always on alert. With this in place KPIs can be set, levels can be measured and improvements can be made.

The same goes for our FileGPS feature. Its "Call Home" capabilities ensure that even if files leave the organization, administrators can see where the file is, can disable it or revoke access, and can get full reports on what transpired.

**Yaron:**
That's why it's pertinent that you're "Beyond DLP". Current DLP solutions are limited. We're ready for – in fact it's sorely needed – the next generation of DLP solutions. Something that goes beyond a one-dimensional view of the external threat, and incorporates the internal threat, training, KPIs and access control.

The important part is to have the visibility and the capability to measure the effectiveness of the product and the training.

Kfir, I can say from my own experience that I am pretty excited about what you and your team created, and the approach you took to solve this difficult challenge. I'm really looking forward to discussing further.

**Kfir:**
And from my side Yaron, it's been a pleasure as always, and look forward to speaking again soon.