

Insider Threats – an Interview with Amichai Shulman, CTO of Imperva

Listen to Podcast [here](#).

Brian Contos: Welcome to the Imperva Security podcast. I'm Brian Contos, chief security strategist for Imperva. If you would like to learn more about this subject and Imperva, visit [Imperva.com](https://www.imperva.com), check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com. Joining me today is Amichai Shulman, CTO and co-founder of Imperva.

Well, welcome to the show, Amichai.

Amichai Shulman: Hey, Brian. It's a pleasure to be here again.

Brian Contos: Amichai, today we're talking about insider threats. I know there are a lot of definitions about what insider threats are, and I don't know if any one's more right than the other. But I'd like to hear from you. In your own words, how would you explain what an insider threat is?

Amichai Shulman: Insider threat is a risk factor that is affected by people within the organization. Now, one thing that we must remember is that an insider threat is not necessarily because of malicious intent, but actually more probably carelessness or negligence. We can see that, for example, with a lot of people working inside organizations taking data outside of databases into their own work stations and laptops for analysis purposes, trying to contribute to the organization, but then when that laptop is stolen or lost, the consequence for the organization is eventually a data breach or data leakage, which is a bad consequence.

I think that still today most insider related incidents are of that nature. But of course there are other incidents that are of a more malicious intentional nature.

Brian Contos: I think you make an important point there about carelessness, negligence versus the malicious insider. What I have found in my experience is the impact at the end of the day could actually be the same, regardless of the insider, to your point, being careless and actually trying to do good things for the organization. Also, during investigations it's often hard to determine early on - did this person do this with malicious intent, or was it an accident?

Amichai, you and I have been thinking about this for a little while. In terms of some examples, maybe you could share some technical, highly skilled insiders or perhaps even some non-technical examples just to show both sides of the spectrum.

Amichai Shulman: Sure, Brian. You mentioned the issue of highly technical attackers, and usually with internal threat attackers, even those with malicious intent are usually not that technical and that sophisticated. The chances of having a hacker inside your organization are dramatically less than having just a malicious person, a disgruntled employee or someone of that kind, which is not that highly technical.

Insider Threats with Amichai Shulman

A few incidents that I did encounter, one of them did require some technical skills where an employee of a cellular provider was actually going into the database of prepaid cards and then putting more money into cards of friends and family through direct entries into the database server.

Actually, this is something that we came across in one of the Secure Sphere pilots. Another incident which shows a little bit of the character of the insider threat is from a previous life where we had an incident of a virus making computers go down in some network.

It was really a weird incident, and it took us a while to get to the point where we actually got to the person who put the virus personally into those computers.

It turned out that this person who had access to the computers did not have the skills to create the virus. He was given a diskette with the virus by someone from the outside who had the skills to create the virus, and all that insider had to do was double-click on the icon file and make the virus run.

So this is what we would expect from internal attackers. In that case, we had an external skill with an internal disgruntled employee that created this kind of attack.

Brian Contos: Yes, those collaborative threats remind me of the attack on Sumitomo Bank in London when a nighttime security guard allowed some friends into the building, and they were dressed as a cleaning crew. They simply walked in, installed some key-loggers. They came back the next day. They gleaned all the access information, credentials, account numbers, et cetera from those key-loggers, and they ended up transferring about \$400 million out of the organization.

Amichai Shulman: Exactly.

Brian Contos: Amichai, there are lots of stats, and surveys, and studies around insider threats, but from your perspective, is it more pervasive than it was five years ago or so? Are we seeing more incidents of fraud, and information theft, and sabotage? Does it feel like we're just seeing more because we're catching more? What are your perspectives on the stats and figures?

Amichai Shulman: I think that in terms of the ratio between insider attacks and outsider attacks, in the past five years we have seen growth in the portion outside attacks have in this question. However, I think that looking at absolute numbers, we do see an increase in insider incidents, definitely around the part of negligence and carelessness.

We also need to remember that the success ratio for insider attacks is much higher than that of outsider attacks, dramatically higher, because it's usually an issue of direct access with valid credentials, some administrative access to an application or a database, and there's almost no issue of not succeeding eventually.

While with outside attacks, you have to find a vulnerability. You have to find your way through the vulnerability, and success ratios are definitely lower.

Brian Contos: You know, Amichai, when you're talking about insider threats, it's almost impossible not to bring up privileged users; system administrators, database administrators, people with elevated levels of trust and access. Is it really possible to control risks associated with a malicious insider that might also be a privileged user?

Amichai Shulman: Well I like the way you phrased it, because this is the way we see it. It's whether you can control the risks. And the answer is yes, you can control the risk. Whether you can absolutely prevent this, no. You can control the risk, you can control the risk by, for example, using security solutions that are independent of the protected systems. For example, if you use web location firewall in front of a web application, you are able to prevent some malicious activities by application administrators.

Same goes for database servers, if you have an independent security solution around your database server, you will be able to mitigate some threats associated with malicious DBAs.

And with that you keep a good monitoring on activity that is carried out by administrative users, by higher privileged users in a way that allows you to detect abnormal activity within reasonable time.

And six months is not a reasonable time, 24 hours is most often a reasonable time to detect this kind of activity. Then you can definitely reduce the risk associated with internal privileged users.

Brian Contos: You know, I really like how you brought up detection in there. Because when a lot of people talk about security, they tend to just move to the prevention side. And I think there are thing that you can for prevention, and you mentioned a few of them. But really when it comes to malicious insiders, what I found is the difference between an insider that's truly malicious and an insider that's simply doing their job is a very fine line.

And very rarely is it a big red flag, but it's mostly a yellow flag. But if you put enough of the yellow flags together, and you look at them, then you have the red flag.

And I've seen this more and more around sensitive data, which appears to be, and I don't think this is anything new to any of our listeners. This is really the new target. People going after data.

Everything from credit card information, and presumably identifiable information, to intellectual property and beyond. What is it that organizations can do?

What steps can they take to really protect the sensitive data when you've got people coming through portals, DBAs, system admins, you've got internal users, partners. It's just everyone's touching your data. How can you really protect that?

Amichai Shulman: Two things about it. One is that not everybody should touch your data. For example; if we take internal administrative users, those usually have to take care of database indexes, storage spaces, structures of tables, and key optimization within the database and so on. They usually don't have to extract data from the database. So if you have a control that allows you to detect when this type of user is actually extracting data, or changing data rather than changing the structure of the data; then this is one risk you can mitigate. There is also the issue of who should be accessing how much of the data.

And if you know that normal application access is usually one record at a time, and then you get to see queries taking hundreds of records at a time from a database server, then this should clearly raise up a red flag in your security solution and so on.

If you know what kind of data is accessed by which users or which class of user, and how much data is being accessed or the access pattern by each user group or user, then you can clearly create a policy that would mitigate insider threats.

Insider Threats with Amichai Shulman

It's not as easy to always know who's accessing what data and how. And this is where technologies like dynamic profiling become very helpful.

Brian Contos: Yeah. And I think you hit on a couple points there. One is knowing where your sensitive data is, where it really resides, what it is. So you can protect it, because if you don't it's almost impossible to apply wholesale security approaches.

Amichai Shulman: Well yeah, that would be difficult I guess.

Brian Contos: And then of course profiling, which I think is probably more critical in addressing threats from privileged users and insiders, than perhaps any other type of attacker. Because you're really looking and baselining how people are interacting with your data; through the application, the application to the database. And you can see anomalies.

And if the average person downloads 12 documents a day, and this person downloaded 12,000,000, well that's anomalous, it might warrant further investigation.

Amichai Shulman: That's interesting example you just brought in, as it relates to an incident from I think two or three years ago of an employee of one of the chemical companies, I don't remember the name right now, who in working for a competitor downloaded thousands of documents with intellectual property.

Brian Contos: Definitely some good content here Amichai. And I think maybe there's even some follow-up podcasts we'll do around this discovery portion, and the classification of sensitive data. So once again, thank you so much for joining us on today's podcast.

Amichai Shulman: Thank you Brian, it was my pleasure.

Brian Contos: If you would like to learn more about this subject and Imperva, visit Imperva.com, check out our [blog](#), follow us on [Twitter](#), or send us an e-mail at blog@imperva.com.



North America Headquarters
3400 Bridge Parkway
Suite 101
Redwood Shores, CA 94065
Tel: +1-650-345-9000
Fax: +1-650-345-9004

International Headquarters
125 Menachem Begin Street
Tel Aviv 67010
Israel
Tel: +972-3-684-0100
Fax: +972-3-684-0200