

Security in a Tough Economy - Don't Let Down Your Guard

With these tough economic times reducing costs is part of a company's survival strategy. But one area SMBs should be careful when cutting cost is Security. Decreasing spending in security can mean increasing the risk of attack.

**Speakers: Michele Ogle, Infrastructure Solutions Marketing Manager
David Puzas, Global Marketing Executive, IBM Security & Privacy Services**

Michele:

Hello and welcome to the IBM Infrastructure Solutions Podcast Series for SMB. This segment is security in a tough economy. Don't let down your guard.

With these tough economic times everyone has shifted into survival mode. Reducing cost is the core to company's survivor strategy and it affects all areas of the business especially the IT department. For most companies investment in areas like business continuity and security end up on the chopping block. But is otherwise decision? We are seeing stricter regulations targeted to better protect customer information and more sophisticated malicious code produced daily. For small and medium businesses where resources and funds are already at their minimum letting down your guard against external and internal threats can prove fatal.

Joining us is David Puzas, Global Marketing Executive for IBM Security and Privacy Services to share some fundamental reasons to keep security at the top of your IT investments.

Hi David, how are you today? Thank you for joining this podcast.

David:

Fantastic, thank you for having me Michele.

Michele:

David you have been in the security field for quite some time now and I know you've seen it evolve over time. What have been the changes in the years that you have been in the business?

David:

As you mentioned I've been doing security for quite some time, a little over 15 years now and I think whether you look back five years or whether you look back five months or even five days, security is one of the things that I have found is always evolving even more so today than I have ever actually seen. When you look at the fact that security is one of those areas where it just doesn't discriminate, it's one of those parts of the industry that when you consider what you have and how valuable the information that people have on their networks is today, regardless of

whether you are a large enterprise or a small business you have to take the necessary precautions to really protect yourself.

When I look at the landscape now it's really shifted from this what used to be this full glory scenario to a full profit scenario. Then you combine that with compliance and the need to extend your business from traditional brick-and-mortar to online types of businesses to take advantage of reducing cost and complexity and operating environments, each one of those things has really introduced and opened up more avenues and doors for what we will say the bad guys to really cause problems.

When I look at an SMB environment the small-business owner nowadays is impacted as much as they have ever been if not more but it also was one of those areas where I think what we are seeing is the growth in this particular part of the business especially the awareness that the small and medium type business owners has nowadays, they are much more savvy than they used to be in this evolving landscape. Definitely when you look at the way things are nowadays with the economic conditions being what they are it is quite interesting.

Michele:

Let's touch on that point around the tough economic conditions. I know you've been in the business 15 years and I know you've seen a couple of tough economic conditions but this one is different. This one is deeper. They are talking depression type circumstances. Why is maintaining security investment at a time like this especially important for our SMB customers?

David:

That is a very good question and you are absolutely right. One of the things that I would really challenge somebody who is considering maybe, to the earlier part of the conversation when you gave the introduction talking about security may be one of those areas that companies consider them reducing some of their assessments. What I would challenge that same customer is they need to look elsewhere and there is a couple of reasons why I say that.

First one of the key reasons is that in a down time much like we are having now what we do see from our big global security operation centers that we have located around the world, we have seen a significant uptake, about a 30% increase in the number of networks and web-based security events that we have seen over the last hundred 2280 days. That's a significant but also I think people forget about that because when you have resource actions and companies are downsizing and budgets are tighter, people also know that companies or the bad guys also know that the same companies that all those people used to work for are going to be struggling with how they really harden and lockdown even the most critical information. When you look at things like credit cards and credit card information being stored on applications and servers and in data centers it now is prime target and prime hunting season for someone who wants to maliciously take advantage of that. Or you may have disgruntled employees and things of that nature. So that's just a mix of internal and external.

That's just one point. The other side of this is compliance. In many organizations it doesn't matter if you're a small company, you're still forced to deal with some compliance mandates that just years ago may not have been something that you had to invest in but due to the nature of the security industry, identity theft, credit card fraud and things of that nature and with this heightened level of interest by the bad guys and the number of attacks that we've seen it's one of those things where you can't just tell your auditor that I'm not going to invest and have it go away or it's not something you're going to deal with this quarter. It's something that you have to continuously maintain a high level of vigilance around organizationally which becomes costly.

Now the mix is how do you actually balance and have you I all this, protect myself but reduce the cost and complexity around my operating environment because security has introduced a significant round of complexity regardless of the size of the organization.

Michele:

Yes David that is probably the fundamental thing out of all of this. Just because the economy has slowed down doesn't mean the hackers and the <malco> developers have slowed down at all. We've got a challenge for SMB, reduced headcount, reduced resources, reduced budget, what particular areas should SMB be looking at to focus on security investments with the limited resources that they have?

David:

That's a good question and I think if you have a dollar and you had to split a couple of different ways what you do know is obviously compliance is one of those areas that you're going to have to spend dollars on. Around compliance the reason why compliance is so critical as an example is all the things that role up under it which are even if you're not having compliance issues to deal with or challenges there are still things you should be very vigilant around making sure that you safeguard and spread your money wisely.

Let me give you a couple of key areas. One is an understanding of the vulnerability in your environment, the vulnerabilities if you will. The ability for you to understand where all the holes, gaps or problem areas are in your network infrastructure and how to determine which ones are the most critical to spend time on trying to address and those that are less critical that can be left for meeting later on but those should be addressed. You have to be able to prioritize that. So that's a critical point, understanding your vulnerability landscape within your environment.

The other piece is all those usually revolve around application. So it's very critical that you focus on your application environment because this is kind of the lifeblood of what you see in many organizations. It's how they keep the doors open, how they process orders and it's how they control inventory. It's how they pushed to the customer what the customer needs to see on a daily basis.

In other instances I think another key area is going to revolve around identity and access especially like all technologies whether it be antivirus or any other type or even identity and

access as an example. The ongoing management cost that an organization has to incur after they have deployed multiple technologies becomes very costly and overwhelming to many organizations especially now when you consider some organizations have really had to make a choice and they have chosen to have to may be downsized or take resource actions which has really strange or burdened the existing staff even further than maybe it was already stretched.

A really good option and one that we are seeing from an IBM perspective is where we have seen a lot of awareness and uptake in our business has been around the acceptance of managed security services by an SMB buyer. I think this is critical and great for an SMB buyer all at the same time. One is it's critical in the sense that they are able to address a very problematic area for them and that security. It's something that they're spending a lot of time and resource time on then this now with the managed service option allows them to get all of the expertise and heightened what I would say better protection at really a lower cost than if they were trying to provide this on their own.

So there is a significant benefit to all the areas where I just mentioned are areas where to focus my investment, understanding my vulnerability in landscape, protection of my critical applications and managing the identity and access control mechanisms that operate within my environment to make sure everybody can do their jobs and can do them efficiently and effectively are all things that can be done using an outsource provider much like IBM and the benefits to the customer is that they are able to save significant dollars in lowering their overall total cost of ownership. They will be able to reduce the complexity in the operating environment. So they're going to be able to get much more out of there existing investments. It's not all about buying more stuff. Sometimes it's all about making what I have worked better, optimizing it for my environment and allowing me to in tern help the optimization of the employee productivity and get more out of what I've got.

All the while I'm creating a heightened level of protection and if compliance is something that you are concerned with your able to demonstrate compliance all through that single shift to an outsourced solution from a provider like IBM.

Michele:

I think these are some really great points and thank you so much. I think when you have made the adjustment and said if I had a dollar where would I put it, I think a lot of our SMB customers are in that particular space. Thank you so much David for sharing your insights and providing some I think very good approaches to security investments for SMBs.

Thank you to those who are listening and joining us for this segment of the IBM Infrastructure Solutions Podcast for SMBs. Remember security threats don't diminish in tough economic times so don't let down your guard.

For more information about IT security and IBM solutions to help you identify and address your security risk areas go to www.ibm.com/expressadvantage/security.