

Risk and Trust – Part Two

Author: Guy Huntington, President, Huntington Ventures Ltd.

Date: October 21, 2010

Table of Contents

Risk and Trust – Part Two	1
Executive Summary.....	2
Registration.....	2
End Point Security and Security Context	3
The Future.....	4
About the Author	5

Executive Summary

Note: I wish to thank Patrick Coomans for asking on LinkedIn why my paper on risk and trust didn't cover things like enrolment, end point security and security context. I was thinking of these when I was writing the paper but didn't want the paper to be too long. Therefore, this paper examines these as well as my vision from more than 10 years ago about how risk would be addressed in future enterprises.

Registration

There are many different identity types interacting with a modern enterprise and identity type gradients for each identity type. For example, the enterprise might have an identity type of "customers". However the type of customer might vary (i.e. the identity gradient). Some may purchase goods and services from the enterprise anonymously; others might belong to loyalty programs while still others might be large enterprises purchasing significant amounts with each purchase order.

Or consider the identity type of "contractor". Some might be accessing sensitive enterprise financial information; others might be working off-shore in a call centre while still others are on-site for extended periods of time, essentially acting as employees.

The risk associated with these identity gradients may vary according to the purchase amount, the type of information flowing back and forth between the enterprise and the identity type gradient, where they are physically based, etc.

In the old days, the way registration normally occurred was for someone who knew the identity to attest to them i.e. saying "Guy's a good person and I recommend you do business with him" or "Guy's a scoundrel who'll steal from you and I don't recommend you hire him".

In today's world, risk determines, in part, the registration requirements for the identity gradient type. For example, no registration is required for individuals who purchase anonymously from the enterprise. On the other hand, large enterprise are required to provide financial records and bank attestations before large purchase orders might be processed where the risk is large. For the contractor example given above, the registration process might be simply for them to provide a government token i.e. their driver's license or something that has their address on it, while others might have to go through some kind of background check.

However, the quality of the token the identity is providing may not be that good. For example, in two large enterprises I have dealt with they had large off-shore operations. Some identities in the off-shore operations would be "bad actors" i.e. they would steal information, not perform their job well, etc. They would then be fired and go to another call centre that also serviced the same enterprise, use a different name, provide false tokens and then continue being a bad actor. In one case, the identity used a false passport that had the same number as another identity.

The quality of the identity token is dependent upon the risk. For many circumstances, government issued tokens are sufficient. However, when there are large fiscal legal obligations or significant security risks then the quality of the token becomes an issue.

Several years ago, I wrote a [paper on identity verification](#) where I proposed that DNA be used to map to an identity (this would work except for genetic twins). Whether or not you agree with my ideas, the challenge, as I see it, is that identity verification will become increasingly more difficult in the future as human genetic cloning comes into existence. As well, I increasingly fear for an identity's privacy as the world digitizes and continues to globalize.

In summary, as more enterprises contract out significant portions of their internal work, and as enterprises continue to adopt the web and sell goods and services globally, all of this introduces new risk to the enterprise which will need to be reflected in the registration process for the identity.

End Point Security and Security Context

At a large multi-national enterprise I worked at 10 years ago, they wanted to have different authorizations for their employees or contractors depending on who they were, what they were logging on from and where they were logging on from. For example, if Guy was an enterprise employee and was logging on from Russia, they wanted him to only be able to do a limited number of functions as compared to him having all capabilities if he was in the office on a secure network. The degree of risk varied by the identity type, the identity gradient, the physical location, the way in which the identity was logging on and the role the identity was playing when he logged on.

In those days, addressing this was very complicated and in most cases cumbersome or extremely hard to create policies that allowed this to happen. The infrastructure required to support this wasn't there. We were just beginning to authenticate devices to the network, we had trouble figuring out what roles Guy was playing, end point encryption was just being implemented and there wasn't a language that could easily create these complex access policies. Further, the firewall security was difficult to set up to allow for all these different circumstances.

Today, the challenge is even larger with content now being able to be accessed from any point on the globe. For example, if Guy is logging on from Russia and accessing a sensitive document, then his authentication requirements might be higher and portions of that document should be omitted or shaded out than if Guy is accessing the document from his office. So now you have content management integrated with identity management integrated with risk management.

There is some good news on the horizon to deal with this. [Axiomatics](#), has a authorization product that is coded from the ground up in [XACML](#) (eXtensible Access Control Markup Language) and [SAML](#) (Secure Assertion Markup Language) that allows the enterprise to write Policy Attribute Access Control. This means that complex authorization policies can now be relatively easily constructed and enforced at the security enforcement points.

However, even with these tools, there is an awful lot of hard work that needs to be done in the enterprise. For example, you can't have enterprise data clouds without having done data classification. This is no small task and requires risk assessments for data.

Tying the authorization policy based on risk to the network infrastructure is also complex. For those enterprise that have total control of their networks, then it's likely easier as compared to those who have portions of their network infrastructure outsourced or, don't have good control over branch or independent business unit operations.

Finally, the finer the authorization policy, the greater the likely impact on operations. Using the example of Guy logging on from Russia, the enterprise might have a risk policy that the identity will only be given limited authorization rights in this case. However, if Guy is the CEO and requires access to sensitive documents and applications, then the operations security team needs to be on call 24 hours a day, able to quickly respond and have risk mitigation processes and infrastructure in place. All of which generally ups the operations costs of the enterprise.

Further, administering the fine grained authorization policies that PABAC (Policy Attribute Access Control) offers will likely become complex as this type of authorization becomes widely adopted over the next five years. It requires significant input and continuous conversations between the security group and the business units who own the content and the applications.

The Future

About 12 years ago I was working at Oblix. I was thinking about the future of risk. I told my friend Derek Small I saw in the future that large ERP's (Enterprise Resource Planning software) would have risk modules. These modules would assess risk from several different perspectives including business, financial, intellectual property and security.

Once the risk was established, I then said the ERP would then create and enforce or coordinate security policies based on the risk. Thus things like physical and logical security authentications would be changed automatically based on risk changes. At the time, I wasn't thinking about content and couldn't foresee things like mash-ups and enterprise data clouds coming into existence. My vision now is that the enterprise risk modules would accommodate these as well as enforce security policies.

Further, I saw the increasing complexity that security would bring to the enterprise. I saw that Boards and senior management would have a very tough time seeing their risk and understanding all the security policies and enforcement across their enterprise physically, logically (and now content as well).

I told Derek that I saw in the future that these policies would be displayed in three dimensions graphically. In my mind I saw a Board member able to call up critical and high risks and then see the interactions of the risk with their physical buildings and security as well as by the identity types who were accessing it.

Today, I am extremely frustrated over the use of text based screens to display access control and risk to an enterprise. I feel this code is written by technoids who don't understand that senior management

and board members want to see the picture in ways they can understand it (a picture is worth a thousand words).

I want to end this paper by not taking a myopic view of things for the future. Most progress occurs in small steps, often in parallel or, invented in other industries for a different purpose.

I can see that that progress is being made with the advent of real time capturing of audit data, the development of the iPad for a graphical way of viewing things, the slowly advancing GRC (Governance Risk Control) and ERP's coming to the security and identity space. The development of protocols such as XACML and SAML will lead to the adoption of attribute policy risk controls.

Content digital rights policy, mash-ups and what [Craig Burton wrote about in his paper](#) (see Risk and Trust for this reference) all will lead to new content security protocols allowing content management security policies to be quickly passed and enforced.

It all comes down to risk and trust!

About the Author

Guy Huntington has been in the identity industry for the last 13 years. He has rescued several large Fortune 500 identity projects and written numerous white papers on identity (<http://www.authenticationworld.com/papers.html>). Guy can be reached at guy@hvl.net or 1- 604-861-6804.