THOMSON REUTERS
ELITE™

WHITE PAPER

CRM AND CLOUD SECURITY
A DISCUSSION WITH MICROSOFT AND THOMSON REUTERS

the answer company™
THOMSON REUTERS®

INTRODUCTION

The steady march into the cloud continues with applications, systems, and data being migrated with increasing frequency and scale to support commercial organizations around the globe. Data related to customer information and customer relationship management (CRM) is not immune to this trend. One recent report predicts that, by 2018, some 62% of all CRM software will be cloud-based.[1]

In the CRM cloud space, Microsoft's Azure platform continues to set the standard for both innovation and security, and serves as the foundation for Thomson Reuters Elite's strategy for secure CRM in the cloud, Elite recently spoke with Rick Weyenberg, Azure Cloud Solution Architect at Microsoft and Anne-Marie Scollay, Director, Technology & Information Security at Thomson Reuters, to explore various dynamics related to CRM in the cloud, as well as discuss how Microsoft is ensuring the security of data on a global basis.

Elite: Is cloud-based CRM as secure as on-premises?

Rick Weyenberg: Cloud-based systems offer a great deal of security. Interestingly, when we talk to our customers about Azure, 60 percent cite concerns around data security as a barrier to adoption. But when they come to the cloud, 94 percent of those customers experience security benefits they didn't have previously on-premises. These are interesting numbers when you think about the offerings that are available on-premises and how much that costs. Having on-premises data centers is a huge cost, as you need specialist staff to man it. You also have to remember that on-premises data centers are easily accessible by whomever is in the building. It is a myth to think that just because the centers are physically present, this somehow makes it safer. In many ways, cloud-based solutions are cheaper to run and just as secure as on-premises. We just have to dispel those myths.

"Interestingly, when we talk to our customers about Azure, 60 percent cite concerns around data security as a barrier to adoption. But when they come to the cloud, 94 percent of those customers experience security benefits they didn't have previously on-premises."

Rick Weyenberg
Azure Cloud Solution Architect, Microsoft

Elite: Why is Azure a more secure option than other alternatives for CRM in the cloud? What are you doing to protect your clients' data?

Rick Weyenberg: Everything starts with the security tools that we have in place and with what kind of physical and logical mechanisms we have in place to protect our clients' data.

The idea of a perimeter is a key point here—both physical and digital. At Microsoft, we have security staff working around the clock at all our facilities. We also have certain set-back requirements that deal with unexpected circumstances, such as natural disasters.

When it comes to physical security, we take the impact our location has on security very seriously. We have barriers on the perimeter that we place, without exception, to stop vehicles and to stop anything from penetrating the physical perimeter. For example, the fencing goes below ground and prevents entry from pretty much every angle.

We have top-of-the-line alarms and security infrastructure to prevent break-ins, and seismic bracing, for instance, which physically protects the data storage.

Our computer rooms themselves are also very safe. Accessing them requires two-factor access control—a biometric and card reader. The facility is also full of cameras to record all comings and goings.

The physical housing of data and its security is a major focus for us.

Elite: You're talking about how Microsoft physically protects the data housing. What are you doing to protect it digitally?

Rick Weyenberg: Protection of the data also extends to the software that we use. We do network isolation to ensure that the data is not accessible. Our competitors don't do this to the extent that we do.

We also have virtual networks, a concept where you can set up a Vnet, which isolates you from an IP addressing perspective. There's also VPN and ExpressRoute connectivity, so we can give our clients secure connection through our data centers by either a traditional VPN connection, which uses IP security or IPsec, as well as an extension of the MPLS connections.

It should also be noted that logical and physical access is restricted to only authorized employees. We also ensure that those requesting access are fully vetted and we actively weed out phishing schemes.

The viability of our security measures is also constantly tested. We have what's called Red Team/Blue Team War Games. We have approximately 2,000 people on a team and they take turns trying to break into our data centers. This keeps our security measures fresh.

Elite: How are you ensuring data security within the Azure network?

Rick Weyenberg: What truly makes us stand out from our competitors is our use of dark fiber—a privately operated optical fiber network. This essentially means that when our clients are communicating within the context of Azure and when their software is talking to other pieces that are in different regions, they are still on Azure's dedicated network. They are not traversing the public internet. This internal network is far safer than broadcasting data over public channels.

"What truly makes us stand out from our competitors is our use of dark fiber—a privately operated optical fiber network. This internal network is far safer than broadcasting data over public channels."

Rick Weyenberg
Azure Cloud Solution Architect, Microsoft

[1] *State of the Cloud Report 2015*, Bessemer Venture Partners

Elite: How do you deal with data security and data residency requirements across the world?

Rick Weyenberg: We operate in 40 regions across the world (and growing), and that doesn't include our government and Department of Defense offerings. Our clients' data does not leave the confines of those regions unless the client has set it up specifically to do so.

Take Germany for example. The data is hosted by Deutsch Telco because of the European Union's requirements; as a result, it must stay in-country. The same goes for France, for Canada, and the list continues because there is a legal requirement to keep the data within regions. However, within these regions, we also offer multiple locations within larger countries as differences in laws may apply. Think east coast versus west coast in the USA, for example. But again, your data is housed within these locations so that it never leaves those additional, cross-location boundaries. This is something that our major competitors may not be doing.

It is also important to note that we never send any client data back out of the region in which it is housed—any sharing is only done within region and within the confines of the law. We make sure that data is isolated and we treat it like anything else within our infrastructure—it is encrypted within our network fabric.

Elite: What is the level of investment that Microsoft is putting into its cloud security offering?

Rick Weyenberg: Let me just paraphrase a statement we made in a recent news article from Reuters: Microsoft will continue to invest over $1 billion annually on cybersecurity research and development in the coming years.
This is an impressive figure and a significant investment in the security of the cloud solutions that we are selling.

It is also important to note that this is just for R&D. If you look at our run rate for security, it is even more than that. It is literally $1 billion just for research and development. That doesn't include operationalization and production. We also have approximately a $15 billion a year investment to support all these different locations and regions. The investment is ongoing.

Anne-Marie Scollay: To put this figure into perspective, the annual revenue of Thomson Reuters is around $12 billion a year. Seen from this perspective, Microsoft is investing one tenth of Thomson Reuters revenues in security. This is a significant and strong investment in the security of the application and what they are selling.

"Microsoft will continue to invest over $1 billion annually on cybersecurity research and development in the coming years."

Rick Weyenberg
Azure Cloud Solution Architect, Microsoft

Elite: What data security certifications does Azure have? What benefit does this bring to the system?

Rick Weyenberg: Microsoft has attained what appears to me to be every certification under the sun related to information security—we have over 60 separate certifications (and increasing). So, we have ISO 27001, which a lot of international corporations are looking at. We've got SOC 2, we've got SOC 1, we've got SOC 3, we've got FISMA and FedRAMP and NIST. You name it, we've got it.

The certifications, from our perspective, are going to be empowering for the legal sector. When you look at the list of certifications, whether it is working with governmental bodies where there is a need for FedRAMP, or if there is a need to comply with an EU-model clause, we have that. This level of certification just doesn't exist in smaller organizations and it allows us to clearly show evidence of our security credentials.

Anne-Marie Scollay: Microsoft has obtained certifications to address most, if not all, customer requirements to attest to and demonstrate that their security controls are appropriate and operating effectively... These are publicly referenceable, which speaks to the dedication in investment that Microsoft has put into building out secure infrastructure. Furthermore, these certifications are performed by independent third parties—it is Microsoft saying "we're secured and here's the third-party evidence to prove it."

"Microsoft has attained what appears to me to be every certification under the sun related to information security—we are approaching 50+ separate certifications."

Rick Weyenberg
Azure Cloud Solution Architect, Microsoft

Elite: Do you think that "cloud" has a negative reputation on the market?

Rick Weyenberg: I think it is important to delineate because cloud is quite a loaded phrase. Let's say, instead of cloud, hosted infrastructure. This is a far easier term to digest as people are already using hosted infrastructure in their day-to-day business. For instance, many clients may use ADP payroll processing. Do they host that software on-site or does ADP do that for you? The likelihood is that they do it remotely—so they're a hosted software provider. So, people will trust them with their payroll but are afraid of using hosted infrastructure to host web apps for instance. There is no difference between this and what the cloud does. It is just that cloud provokes an emotional response and has a negative connotation of "We don't ever want to put our data in the cloud should be," you know? But many already are, and just don't recognize it. Another example is online banking. We all do that with little reservation and that is, in its basest form, a type of cloud solution.

Anne-Marie Scollay: Cloud does have a certain negative connotation. No one ever wants to put their data in the cloud but few realize that they are doing so already. People relate to this stuff on a personal level because it is people that are making the decision to transfer to the cloud and are using it in their everyday lives through the use of platforms like Gmail and Hotmail. So, if it is good enough for day-to-day stuff, why not at an organizational level?

Elite: What advantages does the cloud bring for law firms?

Rick Weyenberg: From a Microsoft point of view, it is the certifications that will be empowering for law firms. Whether it is working with governmental bodies on FedRAMP certifications or having EU-model clauses, law firms benefit from Microsoft's large-scale investment which they won't see from smaller or local providers.

Anne-Marie Scollay: The main benefit for law firms is that there is no need to maintain IT staff and capital budgets to support a cloud-based solution. There is no need to buy all the hardware and refresh it periodically. There is a lot of overhead that goes into purchasing on-premises solutions and cloud can help erase all that.

"The main benefit for law firms is that there is no need to maintain IT staff and capital budgets to support a cloud-based solution."

Anne-Marie Scollay
Director, Technology & Information Security, Thomson Reuters

Elite: What about insider threat? Can you tell us more about that?

Rick Weyenberg: Insider threat is represented by trusted people and systems that have access to sensitive data and systems. One type of access is physical access. Think about the staff coming in and out of a building. Do offices really lock their door 24/7, or do they have an open door with an unmanned receptionist station where people can come and go as they please? Is there a server room? Are the servers in the server room? Because a lot of times you'll find servers stacked up under somebody's desk. Contrast this to the physical security of the data centers that the public cloud runs on, which are built with numerous controls to restrict physical access to the data centers (and the systems within it), not to mention state of the art environmental controls to protect the systems it houses. Due in large part to the scale at which public cloud providers run, they offer a higher level of security, and certainly more external attestations and certifications than even large firms may be able to afford themselves.

Organizations can have a lot of staff that help support the running of an office that may not be known to most people—support staff can be seen as a risk in themselves. This uncertainty can create a risk that can be mitigated by having an off-premises, cloud-based solution.

Anne-Marie Scollay: Over the past several years, the frequency with which data breaches are being reported on the front page of the *Wall Street Journal* appears to be increasing—from major corporations to law firms of varying sizes, no one is immune. Insider threat relies on the human element—whether intentional or unintentional—to compromise data. Part of planning for a move to public cloud includes classifying your organizational data and determining what can, and should, be stored in cloud solutions. Once the data is classified, the next step is to look at who has what level of access to data and under what circumstances, not to mention what they can do with the data that they are able to access. Public cloud providers like Azure provide additional layers of security between their own employees and their customer's data by encrypting what they provision to clients in a way that the public cloud provider cannot circumvent. In doing this, the cloud provider cannot see what their clients store in the cloud, thus providing an additional measure of security to the cloud customers.

Elite: What security advice would you give to law firms who are considering moving their CRM systems to the cloud? What activities should they prioritize first?

Rick Weyenberg: From the Microsoft perspective, I think it is important to have an understanding of data classification and understand how data is curated. At Microsoft, we've got a very simple classification system. This is essentially categorizing information around low business impact, medium business impact, and high business impact. That classification determines who accesses what, when, and why in regards to data.

This classification dictates the level of security and the level of understanding of the hosting environment that supports that data. For instance, low business impact information is something that could easily be hosted in a low-level security platform like a blog site.

Conversely, high business impact data is not going to be exposed to the public internet at all. It is likely to be more intranet-site based and it is probably going to be encrypted. This will mean that there will be encryption measures on the data. Again, the sensitivity of the data dictates how it should be treated.

Having a curation process in place around the data is also important. It is important to understand who has access to it and who is the person that is archiving it or making sure that it is in a secondary safe location. This all needs to be formalized and helps to build an understanding about moving data to the cloud.

Elite: How can the move to the cloud be made as simple as possible?

Anne-Marie Scollay: I do think it is important to be open to the idea of the cloud. Despite the overall fear of the cloud and that emotional response, it is where business is going because it is just more efficient, effective, and agile.

It is always better to start conversations around the cloud from a leadership perspective—from the top down. To achieve success in this, the cloud needs to be framed as an inevitable progression but one that it is possible to have control over. Therefore, it is maybe a case of dipping a toe into the pool with less sensitive data, and slowly ramping up as an organization builds its confidence and knowledge.

The onboarding solution is also key here. Organizations should ask themselves what they want the process to look like and what level of due diligence they want to do on the cloud vendors that they are considering? The move to the cloud is inevitable but it does deserve consideration.

CONCLUSION

It is clear that security for cloud-based CRM systems is a complicated subject. However, with mindful consideration and planning, organizations can benefit from cloud adoption. As we have seen, CRM systems on the cloud are no more at risk than on-premises systems. Misconceptions exist as to how safe cloud-based CRM systems are but users should be assured that the market is seeing significant investment to reinforce the safety measures for these types of systems. The future is looking ever more secure and increasingly turning towards the cloud to deliver the best possible results for organizations and their users. Now is really the time of the cloud.

Rick Weyenberg is an Azure Cloud Solutions Architect at Microsoft Corporation.

Anne-Marie Scollay is Director, Technology & Information Security at Thomson Reuters.