CIO Review India Magazine

ENHANCED FOCUS ON CYBERSECURITY IN THE DIGITAL ERA

By Sachin Dutta, Chief Risk Officer, Canara HSBC Oriental Bank of Commerce Life Insurance Company Limited

Today, we live in a world that seems to be evolving relatively faster as compared to the evolution cycle that any one has seen in the past. When I say past, the point of reference is late 90s or early 2000 which one could argue not really a distant past. Technology is undoubtedly acting as the main catalyst facilitating this evolution. It has helped eliminate boundaries and continues to bring societies, nations, people connect with each other. In fact, the speed of evolution is so fast that the technology has outperformed or outlived its own recent inventions. The transition from technology based solutions to digital solutions and making such solutions easily accessible, has attracted a lot of investors. Analysts and technicians believe that there is more potential waiting to be tapped. So, there is no doubt that we live in a new world that has just begun to realize its potential.

As the world comes closer and becomes interconnected and more convenient to transact and communicate digitally, there is always a threat to its disruption more so when dependency on technology or digital solutions is on the rise and expected to grow substantially. I am sure that all of us had read about worms, virus or trojans during the 90s while pursuing our careers in computers; however the extent of damage these malicious programs can do now has far reaching consequences. This is because of the sheer scale to which any organization operates currently or will do so in future via digital medium. Simply put, this can be one of the biggest threats to any business and overlooking this risk would mean paying damages in the form of cash or probably bitcoins.

The recent "WannaCry" and many more after-variants of ransomware outbreak have not targeted any particular sector. These events also do not appear to have perpetrated with the intent of stealing information, but were majorly done to cause disruption to various businesses by encrypting their information with a key which only hackers knew or had access to. News suggest that healthcare sector in the UK was one of the first ones to be impacted as a result of this. Hence, there is a lethal mix of information security events leading to business disruption. There are other variants of ransomware where the information is stolen and threat given to organizations to cough up mighty ransom failing which the information is made available on public sites/ platforms.

As the landscape of the risk is changing and threat levels currently being raised to maximum, it naturally triggered the Regulators to enhance their vigil on the risk. Particularly in the financial sector, guidelines have been prescribed and continuously refined with the recent ones being issued by IRDAI (Insurance Regulatory Development & Authority of India). These guidelines

are prescriptive and focus on cyber security along with the basics of information security. While the guidelines help insurance companies in base lining their security controls and bringing standardization, but clearly the challenge for the banking and financial sector is to outsmart the next cyber event.

It is equally important to understand the relevance of cyber security from a customer's standpoint. For customers, breach of confidentiality is as good as breach of trust. If not addressed properly, it can easily manifest into a reputational crisis for any organization.

When the situation is complex, sticking to basics can always help. Here, what I believe can help the organizations to develop a better defense system against the ever evolving threat from cyber events.

• Operate on a consistent framework that is not only in line with regulatory requirements but is also mature and forward looking. This is important incase we want to outsmart the next attack. This could potentially become a unique selling point or a key differentiator for our business. Customers would want to do business with us incase they know that their information is safeguarded against a hack or an intrusion. One can always be a market leader in this space; although claiming supremacy in this area requires courage and one must venture out carefully.

• Be aware of what is at risk and where the potential data leakage points exist in the setup. It is important to segregate the high risk areas from the bunch and work towards addressing vulnerabilities which pose a significant threat over others.

• Focus on information exchanged with the partners as often they act as backdoor for leakage of such information. Carefully choose partners on the basis of their maturity in security landscape and expertise in managing security risk. This, as per me must be gating or mandatory criteria for selecting a partner.

• Have a center of excellence pertaining to information and cyber security within your organization. Needless to say that you would need resources with specialized skill set to safeguard the digital borders. Make sure that these resources give an opportunity to enrich and consistently enhance their skill set with time.

• Consistently invest in upgrading the defense systems like firewalls, intrusion prevention systems etc. It's worth an investment!

• Monitor the trends through logs generated by security devices to pick up trends. Factor those trends back to programming these devices with the help of your OEM to build a level of intelligence. Operate to a quick and agile patch management process as any deficiency there could increase the risk of intrusion.

• Inform and educate stakeholders internally to ensure that there is an adequate support for information security agenda points.

• Ensure awareness amongst all staff/ end users on basic security Do's and Don'ts. In my experience, end user often acts as the weakest link in the entire chain who needs to be consistently reminded about the consequences their actions can have, incase an unknown e-mail was to be clicked open or an unauthorized action was to be performed.

• Discourage security over-rides and especially incase of privileged users or users with admin access.

• Implement a cyber crisis management plan and simulate a cyber crisis event within your Company to assess the readiness levels and upgrade basis on the threat perception. Prevention is better but incase crisis happens, we must know how to react, respond and move back to normalcy.

• Just like the bad guys, there are enough good guys or ethical hackers out there who can help you jointly fight this menace. Use their experience to strengthen your defense.

> It is important that we use the concept of artificial intelligence to our advantage while designing security solutions to protect our digital borders and customer's digital footprints

The world as we see today may look very different in time to come as reliance on technology shall increase substantially. Artificially intelligent systems or systems with capability to self-learn are going to be in demand, and they already are! It is important that we use the same concept of artificial intelligence to our advantage while designing security solutions to protect our digital borders and customer's digital footprints. CR