Post new comment

Introduction

Immediately after the first gulf war in the early 1990's the theories of Revolution in Military Affairs (RMA) and Information Warfare were being studied all over the world as a new kind of warfare. During that time, a course on Information Warfare was conducted at the National Defense University of USA. The course participants were from senior officers of the armed forces, representatives of Department of Defence and Department of State and policy makers from the government. Rand Corporation of US was conducting this course.

At the end of the course a cyber war game was conducted. The following scenario was painted:

- There is a major failure in national power grid. Cities became dark.
- A cyber attack on a national financial system takes place. Stock markets crash. Banking system fails. Widespread looting and riot takes place in malls and departmental stores. Panic sets in.
- The national air traffic control system starts malfunctioning. Two aircrafts carrying passenger crashes after collision over the busiest air field in the country killing more than 650 people on board.
- The communication system and the mobile network stops functioning. The mobile handsets start getting weird messages condemning the existing government.
- National transporting network comes to a halt due to a glitch in the server.
- Military command and control network fails, they are unable to speak to each other.
- A national emergency is declared.

- It is still not known who is behind these attacks. The President and the Commander-in-Chief has called for an emergency meeting. He wants you to present your action plan within four hours. What will you do?

This war game was played 25 years back. This was a hypothetical situation at that time.

Manifestation of Cyber War down the Years

A lot has happened since those days. Cyber war has manifested in various forms in the last about 12 years. Some of the examples are given below.

Estonia. In 2007 the Estonian government decided to move the statue of a Bronze Soldier, a painful symbol of half a century of Soviet oppression. It was shifted from the centre of capital Tallinn to a military cemetery on the outskirts of the city. Cyber-savvy Russian nationalist unleashed a distributed denial of service attacks crashing Estonian government websites disrupting banking systems and communication functioning, banks and newspaper.

Operation Orchard. At the night of September 5-6, 2007, Israeli fighter aircrafts destroyed the Al Kibair complex alleged to be developing nuclear facilities with North Korean help in Syria. The air defence network of Syria was made to function as it didn't see the incoming aircrafts by a sophisticated cyber-attack.

Georgia – Russia. In August 2008, Russian troops crossed into south Ossetia. The combined armed assault was preceded and enabled by a multi-faceted cyber-attack against Georgian government and military infrastructure. It was the first large-scale combined armed operations consisting of air, land and cyber.

STUXNET. Stuxnet was the most sophisticated piece of code even written for a cyber attack. Stuxnet was created jointly by NSA of USA and Israeli intelligence. It was designed to destroy the centrifuges used in Iran's enrichment facilities. During 2009-2010, Stuxnet destroyed more than a thousand aluminum centrifuges installed in Iran's underground nuclear enrichment facility at Natanz. Stuxnet is the first cyber-attack designed directly to damage physical equipment.

Aramco. In August 2012, the Saudi Arabian firm Aramco one of the largest oil producers in the world was hit with a piece of malware called Shamoon that wiped out hard disks of 35,000 of the company's computers. It was suspected Iran was behind the attack in retaliation to the Stuxnet attack.

Sony Pictures. In December 2014, North Korean hackers penetrated the network of Sony pictures ahead of its release of the movie 'The Interview.' The movie was about an assassination plot against the North Korean dictator Kim Jong-Un.

Ukraine. In 2015, Russian hackers attacked three Ukrainian regional energy utilities, turning out the lights to about 2, 25,000 civilians, the first known blackout in history ever to be caused by a cyber-attack. In late 2016, Russian hackers hit the Ukrainian pension fund, treasury, seaport authority, infrastructure ministries, defence and finance. They

also hit Ukraine's railway company knocking out its online booking system for days during its peak holiday season.

In June 2017, Russian hackers used a code that was named "Not Petya" which spread to almost 10 percent of all computers in Ukraine encrypting their content with a destructive payload disguised to look like ransomware. Across Ukraine, it shut down banks, ATMs, Point of Sale systems, paralyzing nearly all the country's government agencies and crippling infrastructures like airport and railways, hospitals, post offices. Later the 'Not Petya' spread all over the world causing the loss of at least $10 billion.

In June 2019 Israel carried out a kinetic attack on a building at Gaza because it was base of an active Hamas hacking group. It was perhaps the first use of real time kinetic response to digital aggression.

In June 2019, the Trump administration retaliated against Iran's downing of a U.S. $240 million U.S. military drone with a cyber attack on a Revolutionary Guard (IRGC) database. The attack wiped out an IRGC database which was used to plan attacks against tankers in the Persian Gulf. President Trump disclosed that he called off an airstrike after he heard about the potential casualties it might cause. The US government carried out cyber operations as a retaliatory measure and not a kinetic action against Iran.

Indian Scenario

Cyber war game as a table talk exercise is conducted to ascertain response options of various stakeholders who maybe under cyber attack. In today's scenario in Indian conditions the following scenario may be played up:

- The Indian railway reservation system is under cyber attack. The central servers have gone down. There is a widespread chaos in railway stations as no reservation chart is available.
- There is a national power grid failure because of sudden lowering of power factor below acceptable level. There is large scale power failure across the country. Transportation like railways, communication systems are adversely affected.
- Highly proficient hackers have broken into cyber defences of India's leading public sector bank, stolen complete accounts data of customers, paperwork of several high profile corporate bankruptcy processes, inter office communication have been compromised, extremely confidential information valuable to any competitive banks have leaked. The extent of damage is still not known but the crisis is unfolding rapidly. What should be the crisis response mechanism of the bank and the government?

There can be many such scenarios. For the sake of discussion, only one particular sector is being analysed in detail here. Let's take financial sector.

The financial sector is the most lucrative target for cyber criminals and is consistently under attack.

In 11 August and 13 August 2018, hackers managed to transfer over ₹ 94 crore through a malware attack on the server of Pune-based India's oldest Cooperative bank Cosmos Bank. Bank's ATM switch server in Pune was hacked and details of multiple Visa and Rupay debit card owners were stolen. On August 11 these were used to carry out around 12,000 fraudulent transactions across 28 countries. On August 13th another malware attack was launched on the bank's server. A SWIFT transaction was initiated to transfer funds to the account of ALM Trading Limited in Hanseng Bank, Hong Kong. Cosmos Bank had to close its ATM operations and suspend online and mobile banking facilities.

A panel of experts was appointed by the UN Security Council to study various UN sanctions breached by North Korea. It found that the cyber attacks on Cosmos Cooperative Bank, was "motivated" by North Korea.

This report came seven months after the malware attack on the bank. [1]

In February 2018, about $2 million was stolen from City Union Bank accounts after a cyber attack compromised the SWIFT messaging system with payment instructions being sent to other banks in multiple jurisdictions. The bank could detect the transactions while reconciling accounts. Fortunately about half the money could be retrieved.[2]

On February 4, 2016 unknown hackers used SWIFT credentials of Bangladesh Central Bank employees to hack and took out $81 million from accounts at Bangladesh Bank. A type mistake prevented the hackers from stealing the full $1 billion they were after. $81 million via four different transfer requests was sent to Rizal Commercial Banking Corporation in the Philippines by the hackers. The money was deposited into four accounts at a Rizal branch in Manila on Feb. 4. The $81 million that went to Rizal Bank in the Philippines was gone.

This is an entirely feasible scenario. The various issues are discussed in succeeding paragraphs.[3]

The moment a cyber breach is detected, the technical people get into action straight away. However, it is very difficult to ascertain at that time how much damage has taken place. The problem is: market will come to know something is happening. How much to divulge, who should give out the information and who should be in-charge in handling the situation is the key.

What is the cyber crisis management organization of the bank? What are the critical processes? How much is the risk appetite and tolerance? What is the business continuity plan? The leadership should have a clear plan as to how to deal with these problem.

Information flow inside and outside the bank has to be handled in a controlled manner. If not handled correctly, it has dangerous repercussions. What is the bank's public relations management plan? Who will brief the media? It is preferable that the executive head briefs the media. He/she should have had developed enough confidence with the media earlier so that it doesn't appear as a sudden appearance.

Who does the bank alert about the incident? Clients should learn of the incidence from the banker itself. Should be done as earliest as possible.

Normal tendency is to handle the crisis at the bank's own level. This has dangerous consequences. If the information is passed on to others the other banks can take remedial action so that crisis is controlled.

What is the role of regulators when notified? Will the business people of the banks start talking to customers about what is going to happen and analyse the state of affairs of the bank?

As per GDPR rules the bank has to inform the regulator within 72 hours after knowledge of an incidence. If you do not do, the fines are huge as the percentage of profit and has serious consequences. What is the rule position in India? The banks have to deal with the technical, business, security, reputational and image crisis at the same time. Who is handling what?

In the event that customer's confidential data has been compromised, when should the bank learn of this fact? There is a delicate balance between how much time you need to understand and how quickly you need to inform the customers. There is a need of a right balance that is difficult to attain.

What should be the management's first decision options? Options are:

- To disconnect the bank's network completely from internet, isolating and halting all operational system.
- To disconnect critical systems that will affect business functionally.
- Leave the system connected to allow for a full forensic analysis.
- Ask business continuity manager to present the cyber crisis management plan before making any other decision.

Ideally, bank should be able to continue business, deal with the crisis and everything should go parallel.

Three months later when the bank feels that the storm is over, damage control systems are in place, security holes are being patched and cyber experts have enough defensive measures to give banks some respite disaster strikes again. On Monday morning, there was a report of dozens of unauthorised SWIFT transfers totally $330 million from the bank's account. The IT people, lawyers, law enforcing agencies and the management scramble for recovery. Details of attacks have been leaked to public. Somebody like 'Anonymous, We the trustees of Globe' announces as yet another demonstration of their ability to do what they will do with global financial system. "Today it is a bank's turn as key player in the elitist corrupt banking system." By end of the day rumours have taken over. Media accessed to leaked internal communications between bank's senior officials, embarrassing mails including irresponsible, angry slander showing lack of professionalism, debate about how the crisis was handled with press leaks trigger waves of investment withdrawal requests. Foreign firms have no trust and confidence in

banking systems and search for alternative investment opportunities.

IT people find that attackers found a hole in the software of the bank's critical contractors. Same contractors provide services to a large part of banking industry. It may cause devastating affects in the entire banking industry potentially harming country's financial stability.

Supply chain issue. The suppliers of software is an exclusive club. Lot of same software is used by different banks. What is the policy to deal with such suppliers? Procurement plan need legal steps to deal with such a situation. Suppliers are to be informed which may help competitors, may affect entire financial system.

What is the most significant effect of media reports in times of crisis?

IT people must continue to mitigate issue, management pushes technical people to provide answers which might not be there.

Who should represent banks for public announcement? Bank CIO, most senior responsible for IT, bank's spokesperson or third-party crisis management expert or highest executive as chairman of the board?

If you are the CEO of a competing bank, what actions will you take? Recommended options are:

- Inform the media that such a scenario for your bank is unlikely to occur. Inform the public that the bank takes the event seriously and is working to learn the lessons. Stay quiet, do not relate to the event in any way in order to avoid confrontational dialogue. End the relationship with that suspected suppliers thereby preventing customers from accessing critical services. Do not criticize others; may happen to you also, take the event seriously, have a plan not necessarily a perfect plan.
- Trust with customers, how fast to brink bank services, background, forensics?
- Planning is key. Train people to handle such a situation. Plan is nothing, planning is everything.

Conclusion

Normal routine cyber security measures provide inadequate defence against sophisticated attacks. Organisations need to build confidence in their ability to recover rapidly and resume normal operations. One of the methods is carrying out the war game to examine how a critical infrastructure responds to realistic simulated cyber crises, effectiveness of its contingency plans, under which conditions they are more likely to fail and how it enacts & adapts business continuity plans. The war game tests, technology, processes and procedures, through the phases of identification, defence, response and mitigation. To enable organization to review and develop the personal and team skills required to coping with cyber crises the war game allows observation, monitoring, feedback and mentoring, War games test resilience and build capability.

It is clear that the ability to resist, react and manage such attacks requires an effective

combination of technology processes and managerial procedures. At the end of the war game review of different groups' performance and self-assessment, reporting on the effectiveness of technology and methodologies and feedback on the following issues should be analysed threadbare:

- Situation Awareness
- Crisis Management response processes and procedures.
- Decision Making and Decision Taking chain during crisis.
- Risk Assessment Methods.
- Communications: Internal & External. Reaction to public events and media handling.

Cyber war game is a good method in checking capability of organizations to handle emergency and cyber attacks. More of these exercises should be conducted at various levels to constantly upgrade the cyber defence mechanisms of organizations.

Endnotes

1. Rashmi Rajput, UN Security Council panel finds Cosmos Bank cyber attack motivated by N Korea, Mar 27, 2019 available at : https://economictimes.indiatimes.com/https://economictimes.indiatimes.com/industry/banking/finance/banking/un-security-council-panel-finds-cosmos-bank-cyber-attack-motivated-by-n-korea/articleshow/68589549.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
2. Saloni Shukla, Shilpy Sinha, City Union loses $2 million in cyberattack, retrieves half, February 17, 2018, available at : , https://economictimes.indiatimes.com/industry/banking/finance/banking/city-union-loses-2-million-in-cyberattack-retrieves-half/articleshow/62956557.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst
3. Cyber Security – Simulation, War Game, You Tube video available at: https://www.youtube.com/watch?v=FsZqgXw0oeA

(The paper is the author's individual scholastic articulation. The author certifies that the article/paper is original in content, unpublished and it has not been submitted for publication/web upload elsewhere, and that the facts and figures quoted are duly referenced, as needed, and are believed to be correct).