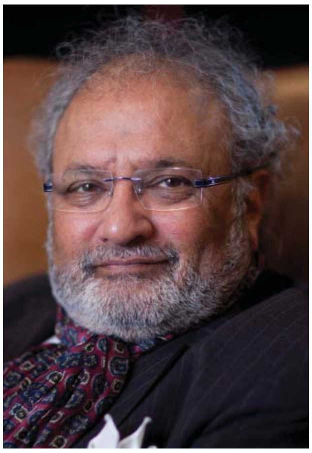
Cybercriminal Actions always have a Purpose; a Ransomware Attack is One



* Kersi F. Porbunderwalla

Addressing the IT-, and Cybersecurity risks are extremely important because an IT Security Manager or a CISO must be *lucky* all the time, while a hacker should be lucky only once. After a significant cyber-attack, all companies say that they reacted quickly to the cyber-attack, which means that the attack was contained, but most surveys show that management is unaware on who can connect and infiltrate the systems, which third parties have access and a commitment to IT governance and the cybersecurity training and awareness as a compliance exercise.

After a cyberattack, most companies in their communication to the stakeholders calm them by saying: the company plans to further strengthen its IT- and Cybersecurity processes. In this blog, we look at the steps to take to avoid a considerable breakdown due to a cyberattack.

Cyber-attacks are an increasingly expensive affair for all companies, which are exposed to targeted attacks all over the world. This added focus has companies to look at the physical and monetary resources, tighten up the security budgets and look at the options of buying cyber insurance when a hacker attack has paralysed the IT systems across locations and business units.

Ransomware to seize data and hold it as a hostage

In spite of the attention, the financial consequences for a company that cannot function in the usual way for a period, can estimates the loss in the millions and billions of Euro, dollars or any other currency, while it costs a fraction of the damage, to ensure topical and timely holistic IT and cybersecurity.

Ransomware attacks are a top priority, and so is spear-phishing and similar attacks. Unfortunately, due to the long-time this criminal activity has flourished, ransomware is now a global big business, and the criminal attackers are uncompromising in their search to develop new, creative ways to infiltrate the corporate networks and IT environments. The Boards responsibility is to ensure that the company IT platform(s) are resilient and can restore operations at scale if there is a significant breach. One simple possibility is to use the cloud, applying a hybrid approach that combines on-premises infrastructure with multiple cloud storage vendors.

Document and demonstrate that reasonable technical and organisational processes were in place

When a critical IT incident/attack occurs, it usually closes all IT systems across locations and business units. The lack of access to IT systems has had consequences for crucial business processes throughout the value chain and everything from production, logistics to distribution is affected making it impossible for the organisation to do business at normal levels after the attack, which affects the reputation, sales and can also cost fines from the oversight authorities if the company cannot document and demonstrate that reasonable technical and organisational measures were not taken to prevent a cyber-attack.

Several vendors provide a more or less straightforward, and secure IT and data backup solution. The service restoration must include a comprehensive data protection solution to protect against the potential attack and restore the backup and recovery infrastructure. The repair and recovery must ensure that the production environments are up and running in spite of the attack.

To do that, management of the infrastructure has to be designed and optimised provided by the optimal data protection and recovery tools. These must be able to combine and integrate with multiple cloud vendors to be on the safe side so that all systems and servers will be up and running again within the next two to three hours instead of weeks.

Ransomware, spear-phishing attacks are quite simple to execute

Not all attacks are made public, and the media interest is limited unless the cyber breach is magnanimous. Some of the recent attacks that cost a three-digit million number are Maersk, Norsk Hydro and Demant, to name a few recent attacks that were made public in the Nordics.

Access to the systems starts in most cases with something as simple as, a phishing email that causes an employee to download a document or spreadsheet. It can give hackers access to a network. During a ransomware attack where the data gets encrypted and make the content inaccessible and de-encrypted only if a large amount of money usually in bitcoins to avoid a trace is given so that the company can regain control over the systems again has the minimum consequences:

- The company has to switch to manual operation for some time
- The website is out of service as a result of the attack
- Employees cannot turn on the computer
- Production facilities are shut down
- Besides reputation damage, industrial espionage is another disaster
- Broken IT systems and infrastructure after the breach

In the latest assessment, the Defense Intelligence Office writes; it seems that cybercriminals are always on the lookout for financial gain. Ransomware and ransomware attacks are a top concern for enterprise customers today. Ransomware is big business and attackers are relentless in their pursuit to develop new, creative ways to infiltrate corporate networks and IT environments to seize data and hold it hostage.

No excuse

Therefore, addressing the above issues must be delivered through, e.g. a scenario planning workshop/exercise to address the above questions and find the optimal in-house solutions. Some of the other activities to address all of the above problems is to integrate and embed the resolutions while implementing, executing, monitoring, documenting and demonstrating that adequate and reasonable technical and organisational processes are addressed in the daily routines and operations of Data Privacy, Protection, GDPR, IT- and Cybersecurity procedures. ■

***Mr. Kersi F. Porbunderwalla** *is the President & CEO of the Information-Security Institute, and The EUGDPR Institute, and Secretary-General of Copenhagen Compliance, Denmark*

IOD's
MSME
DIVISION

Helping you grow
Uninterrupted

I am happy to note that, the **Institute of Directors**, a pioneer institute for professional development of corporate India, has taken the initiative for hosting capacity building programmes for **MSMEs in India**

RAM MOHAN MISHRA, IAS
Additional Secretary & Development Commissioner
Ministry of MSME, Govt of India.

IOD's MSME division envisions providing a holistic platform to facilitate growth and competitiveness of the MSME sector. It aims to become a pioneering body for the professional development of the MSME sector, especially the thriving start-up enterprises.

At IOD, we appreciate the diversity and the challenges that MSME's bring and we aim to address them through a portfolio of activities spanning from training to specialized award system.

IOD's overarching position to create synergy among various facts of the MSME sector will effectively promote the following:

- Networking and Interactions at conferences, seminars and workshops
- Research and documentation on MSME Practices
- Conduct training programmes in MSME clusters
- Certificates awarded to appreciate professional competence

THE MSME FACTSHEET

- Over 30% contribution to GDP
- Employing more than 11.1 crore people
- Over 78% rely on self-financing to meet their credit requirements

Certificate of Participation
Will be issued on successful completion of course.

MSME spotlight

Subscribe Today
IOD's Monthly Digest
underscoring the MSMEs
and their expanding frontiers

INSTITUTE OF DIRECTORS
M-56 A, Greater Kailash Part - II (Market), New Delhi -110048, India • Board Nos.: +91-11- 41636294, 41636717, 41008704
Fax: +91-11- 41008705

For more information, please email: **info@iodglobal.com**

www.iodglobal.com