Summary of EY GISS under Cyber Attack Survey.

GISS is an acronym for Global Information Security Survey. According to EY, a global organization, Cyber Security is becoming more essential than ever, and needs to be realized by everyone in the world, whether in the IT sector or not. When cyber criminals strike, it is not just IT departments that suffer. The ordinary farmers or traders will find bank systems not working, thus agriculture, trade, fishing and even tourism will be deeply affected. Cyber attackers keep changing tactics, doubling persistence and widening attacking capability, and cyber-attacks keep evolving and the threat only gets bigger.

The Internet of Things (IoT) is greatly a potential exploit of cyber-attacks. Humans and devices have never been so closely connected before in history, and even more advanced. Machines are equipped with great processing and communicating power, learning capabilities and some human-smart behaviors. We however cannot assume the fact that networks are used by cyber criminals to intercept information as devices communicate. In all the chances, we have an individual ahead of the machine, who can decrypt any encryption, and even change the information without detection. IoT’s integration into delicate fields such as health and banking services means that the communicating devices need to be secured.

Cyber threat Intelligence helps firms to continually gather, and analyze threats in cyberspace, thus help security personnel get ahead of cybercrimes by gathering some intelligence that can be used to get the criminals before the crime. A firm can decide to come up with a CTI program, through EY, which supports its affiliated firms in maturing the processes and make them more

robust. EY also helps clients shift focus from data and comes up with a quick intelligence model. It also takes an expertise look into their client’s threats and explains what needs to be done before what to achieve success. Due to advanced systems and security focus, EY also helps the client with choosing most suitable technology. All information sharing opportunities are also identified.

Away from fighting cybercriminals, EY goes ahead to help clients in insurance section. The clients need help in lost estimation procedures. EY team contains accountants, finance experts as well as technological staff members. It will thus determine what really happened, then go ahead to decrease the timeframe for claims procedures and cash provisions. EY will also help a client in claim development and submission, with the goal of taking note of the maximum number of loss risks. Lastly in insurance, EY does claims resolutions, trying to make the claim decision make sense to the client, coming up with alternatives and representing them to the insurers.

When fire starts, let’s say at building A, the greatest cause of damage is that resulting from delays in response. When attackers begin an attack, each minute they spend in the system is a minute of privacy break. EY uses a Cyber Breach Response Program (CBRP). The CBRP then becomes the focal point of a variety of stakeholders needed to solve a breach. The kind of management allocated to the CBRP is a major determinant to its success. In EY. The managers are always people with great legal, compliance and technological experience. Such a team will easily gather attack details from the clients if they happen, and above all, will be on the wait for any attack, thus give better services.

EY may be seen as a solution to cyber-security issues worldwide, as new trends come in, their services are becoming more and more useful. To solve this issue, however, we all need to join up, come to a common understanding and work by the same.