I J C T A, 9(17) 2016, pp. 8623-8628

Security Against Cyber Attacks in Food Industry

Afsha Khursheed[*], Mohit Kumar[*] and Monika Sharma[*]

ABSTRACT

Food Industry has seen highest growth rates of all times in recent years. This paper focuses on the alarming rate of increase in cyber-attacks on the food industry. We emphasized on the major threats that the industry has come across recently and loopholes of the regular clichéd system in this industry. We have also focused on major cybersecurity breaches in the history and some recently developed new job profiles which deal with the issue, thereby minimizing the risk of cyber breaches and making the industry flourish like never before.

Keywords: Security, Cyber Attack, Cyber Crime, Supply Chain

I. INTRODUCTION

Security has been an issue of utmost importance, ever since the beginning of digital technology. Hackers have been seeking confidential data through new methods of entry into servers. Although, most of us do not relate food and beverage supply chains to such security threats, this sector, however, is in the forefront ofthe cybersecurity community, according to the recent trend in cyber-attacks. The National Cybersecurity Institute stated that the "Department of Homeland Security has labeled the Food and Agriculture industry as one of the 16 national critical infrastructures." these organizations are clearly at an alarming risk to such attacks than any other sector. When talking about the food and agriculture division, the issue lies with "agro terrorism".

Forbes defined agro terrorism as the "intentional contamination of the food supply with a goal of terrorizing the population and causing harm." [1] Agro terrorism can work on two levels. Firstly, the Hackers can sneak into the major supply chains and interrupt the transportation of goods wherever the food is needed. This can have catastrophic effects because it can completely cut off the supply of food and beverage of any place. Secondly, the hackers may gain access to certain programmable logic controllers and could interfere in the process of food irradiation, thereby giving them the authority to intervene in the amount of chemicals being put into the food leading to human sufferings, illnessandpotentially, death. Imagine if your favorite foods posed a threat to you. That makes the issue of cyber security a concern when it comes to food industry.

The International Business Machines Corporation (IBM) conducted a research in 2013 which was led by their security services department and it aimed at analyzing the vast number of security breaches and similar incidents on any of the systems that their clients used and it helped to uncover that annually they faced an average of 73,400 attacks. Further analysis indicated that most attacks were targeted at the manufacturing industry, food industry being a part of that, following it were the insurance and finance industries. [2]

[*] Amity Institute of Food Technology, Amity University, Noida, Uttar Pradesh, India, *E-mail: Afshakd@gmail.com; Itsmohitk@gmail.com; Msharma5@amity.edu*

1.1. How is cybersecurity related to all of this?

One would think that why is cyber security needed in food industry, or any other manufacturing industry for that matter. Manufacturing industries don't handle credit card details or high level finances and there are not many secret documents that are kept or shared over the internet so why do we need to concern ourselves with it? It's because as an industry, the threat lies not only to the present state of what the industry makes, but rather where the industry is headed in the future is also what an attacker might be after as well. Trade secrets and goodwill are some of the factors that affect the future of any specific firm in an industry and cyber security is needed for the safety of these factors so as to further the cause of that industry as a whole.

Automation is becoming an essential element in the food industry with the development in computers and robotics. Many stages in the food production and processing line are handled by machines and it is optimizing the efficiency of the processing methods and saving time as well. Automation can be seen in many of the food processing industries. For example the dairy industry, As per Lely, which is a worldwide maker of agricultural machines, half of the dairy crowds in north-western Europe will be milked by robots in 2025. [3]

Up until 2010, it was a common belief that cyber threats were limited to office and administrative environments. However, the recent years have proved that it's not. There are malwares such as Night Dragon, Flame, Stuxnet and Dugu that have targeted and affected industrial automation systems. [4]

Food Quality and Safety reported that cyber threats to food and beverage industry are extremely dangerous for all of us. Uncertain remote access, frail security setups, obsolete firewalls, carelessness, working framework blemishes, untrained staff, imperfect security strategies, and poor change control systems are significant zones of digital shortcoming in the nourishment and refreshment store network.

II. MAJOR CYBER ATTACKS IN FOOD INDUSTRIES

- There have been a number of recent large scale cyber-attacks on businesses. In the US, supermarket Target was subject to an attack over the Thanksgiving season. Hackers stole data from up to 40 million credit and debit cards of shoppers over the busy holiday period. More recently White Lodging, a company that manages various Hilton, and Marriott hotels, reported that a cyber-attack had occurred in the restaurants and bars of 14 of its locations across America, exposing the credit and debit card details of customers. [5] The recent breaches of Cafe de Coral and Biggby Coffee demonstrate that cybercriminals are not just attacking point-of-sale systems, they are attempting to hack any weakness they can find.
- The multinational company Subway was also a victim of cyber-attacks. In 2012, two Romanian men admitted to participating in an international conspiracy that hacked into credit-card payment terminals at more than 150 Subway restaurant franchises and stole data for more than 146,000 accounts.[6]
- Dairy Queen, a chain of soft serve ice cream was also victimized by cyber-attacks. In 2014, the credit card and debit card details of the customers of nearly 400 Dairy Queen and Orange Julius stores were compromised in a cyber-attack by a third party back off malware which was infected through a third party vendor's stolen account credentials. [7]
- The restaurant P.F Chang's China Bistro faced a similar incident in the September of 2013 and June of 2014 when the credit card and debit card details of 33 restaurants of P.F Chang were compromised and sold on the internet, like many other victims of similar attacks.[8]
- The attackers are not only targeting the personal data of customers but they are also stealing the intellectual property, copyrights and other creative works of the major market players.

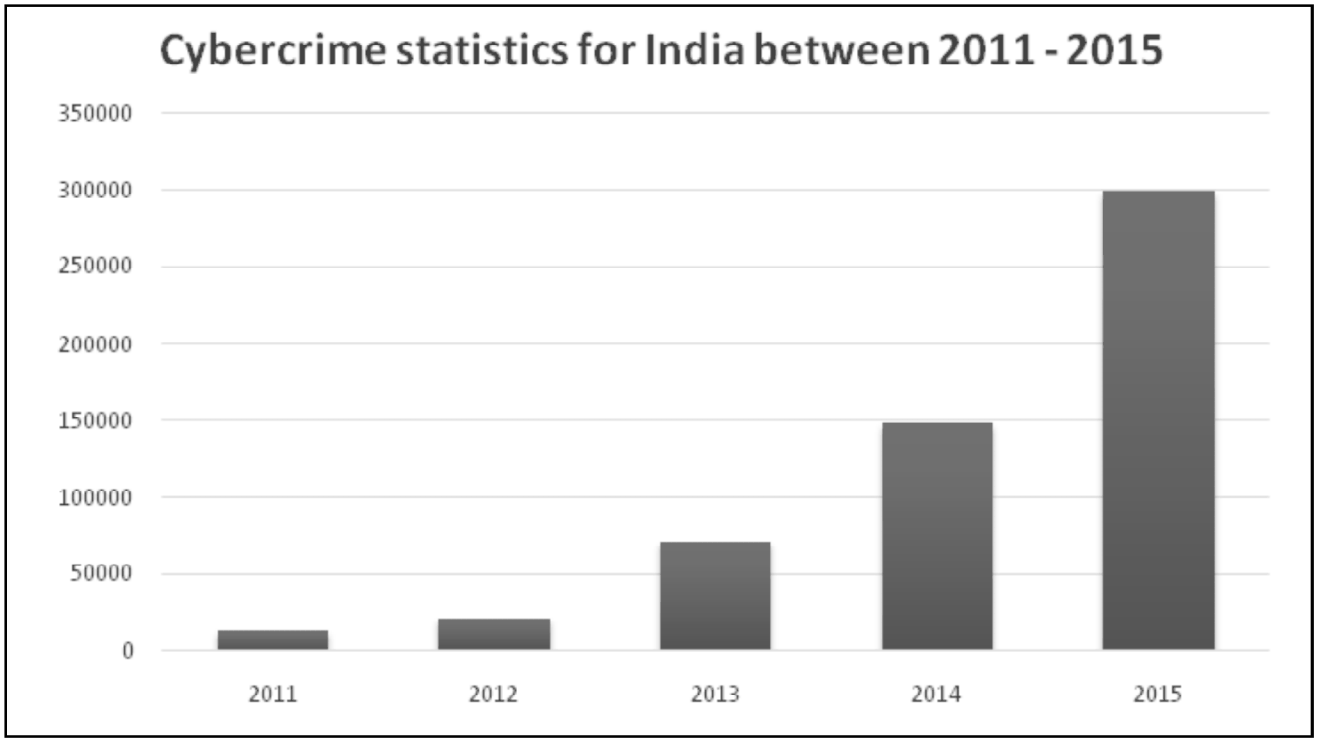

Figure 1: Cybercrime statistics for India between the years 2011 to 2015 [9]

Also, the Global Security Report by Trustwave (2013), confirms that, the 24% share of the total data breaches occurred in the food and beverage industry alone and it continues to be the most likeable target with the retail industry. The reason being, most commonly, the standardization of systems. For instance, if any security deficiency exists in a specific system, then, it is most likely to be duplicated across the entire network, thus, leaving the entire system susceptible to a cyber attack.

III. SAFETY ACHIEVEMENT AGAINST CYBER ATTACKS

Considering the weaknesses mentioned above, improving the cyber security in the food and beverage industry can help us all fight the cyber terrorists from infiltrating into the supply chains and creating grieve problems for the nation. For this, each and every organization involved in the food and beverage supply chain needs to employ well-trained cybersecurity professionals, so that their systems could get scrutinized for weaknesses and the software security can be maintained. Such professionals can also outrun any other chances of cyber-attacks possible. The less control the hackers can gain, the safer the food supply is.

There are certain job profiles which owe cyber security to their respective organizations and play certain vital roles in attaining and maintaining the cybersecurity. Few of them are discussed below, in context with their roles and responsibilities. [10]

3.1. Chief Information Security Officer (CISO):

A CISO is the official level director who gives guidance to the methodologies, operations and the monetary allowance for the administration of the endeavor and its assurance. The responsibilities would include

- Supporting and coordinating the configuration of security frameworks.
- Guaranteeing and testing the business progression arrangements and calamity recuperation.
- Supporting and inspecting the digital controls, approaches and digital assault reaction arranges.
- Approve access and personality approaches

- Survey examinations after assaults or breaks, including suggestions and effect investigation for comparable dangers
- Keeping up a comprehension of the IT danger situation of the business.
- Keeping up consistence with the appropriate directions and changing laws
- Guaranteeing a well-sew inside correspondence framework in the venture among all the faculty and authorizing the consistence.
- Dealing with all groups, workers, temporary workers and sellers required in digital security; this may incorporate contracting, preparing and coaching them.
- Maintaining a constant change in digital security and danger administration system to influence new innovation.

3.2. Cyber Security Specialist

A cyber security specialist in an association attempts to keep their data frameworks secure by figuring out who obliges access to which data, and afterward plan, arrange and implement digital security programs. They are essentially the conduit filters of every last data that is dealt with in the association. Their selective parts include:

- Distinguish and resolve matters identifying with impressive harm through intrusion of administration, licensed innovation robbery, system infections, information mining, money related burglary and burglary of delicate client information.
- Disallow digital wrongdoing by observing and diagnosing malware occasions and dangers utilizing capable investigation, legal sciences and figuring out.
- Plan firewalls, screen utilization of information records and direct access to secure data and system.
- Stay overhauled on most recent infection reports and secure systems from them is a noteworthy obligation.
- To prepare clients and make mindfulness among the association's work force.
- Encourage the administration and official staff with the most recent overhauls and reports.

3.3. Cyber Security Analyst

The job of a Cyber Security Analyst is to detect and prevent cyber threats to an organization. This is done in the following ways:

- Plan, implement and upgrade security measures and controls
- Set up arrangements and conventions to secure computerized records and data frameworks against unapproved access, change and/or obliteration
- Maintain information and screen security access
- Perform powerlessness testing, hazard examinations and security evaluations
- Conduct inward and outer security reviews
- Anticipate security cautions, episodes and catastrophes and diminish their probability
- Manage system, interruption location and counteractive action frameworks
- Analyze security ruptures to decide their main driver-Recommend and install appropriate tools and countermeasures
- Define, implement and maintain corporate security policies
- Train fellow employees in security awareness and procedures
- Coordinate security plans with outside vendors

3.4. Cyber Security Consultant

A consultant is required tooutline and actualize the best security answers for an association's needs. The obligations of a consultant are:-

- Determine the best approach to secure PCs, systems, programming, information and data frameworks against any conceivable assaults-Interview staff and heads of departments to determine specific security issues
- Perform vulnerability testing, risk analyses and security assessments
- Research security standards, security systems and authentication protocols
- Prepare cost estimates and identify integration issues for IT project managers
- Research and outline powerful security structures for any IT anticipate
- Test security arrangements utilizing industry standard examination criteria
- Deliver specialized reports and formal papers on test discoveries
- Provide technical supervision for (and guidance to) a security team
- Define, execute and keep up corporate security arrangements
- Respond quickly to security-related episodes and give an intensive post-occasion examination
- Update and upgrade security systems as needed

IV. CONCLUSION

Recent and rapid developments in technology have revolutionized the food and beverage sector, such that the application of technology is now fundamental to decide the success or failure of the businesses. However, these technological advancements have increased the risk of frauds and cyber-attacks. Hence, to get the best results out of every new aspect of technology, cybersecurity is of utmost importance. Although, the major concern for the industry is securing the customer's personal information, yet the chances of other data breaches and attacks cannot be ruled out and need to be taken care of seriously. With the growing frequency and solemnity of the attacks, certain job profiles discussed are a good and a benchmark solution in today's time. These professional personnel can provide a strong and secure structure to the organization to avoid and/or handle any situation of a cyber-breach.

VI. FUTURE SCOPE

The endless possibilities of growth and development in the food sector can only be brought by preparing the organizations to avoid and, at the same time, withstand any potential chances of a cyber-attack. Therefore, the vision includes the cyber security threat landscape, the technologies which may be employed as well as the practice approaches which may be applied by security professionals. The nature of cyber threats will evolve as rapidly as emerging technologies. A new generation has now had time to re-envision the rules. Cyber threats have matured and now will move towards ever greater sophistication. This is a challenge for successful corporations and emerging businesses because a threat to confidential data can slow down their growth. So, awareness and countermeasures for tackling such threats need to be stepped up. In this modern world, the role of cybersecurity is centralfor industrial growth.

REFERENCES

[1] Cybersecurity in Food - Food Quality & Safety. (2014). Food Quality & Safety from http://www.foodqualityandsafety.com/article/cybersecurity-in-food-and-beverage-industry/.

[2] "The Cyber Threat". Foodengineeringmag.com. N.p., 2014. Web. 2 Aug. 2016.*http://www.foodengineeringmag.com/articles/93155-the-cyber-threat*

[3] Beekman, J. and R. Bodde (2015). Milking automation is gaining popularity. In: Dairy Global. *http://www.dairyglobal.net/Articles/General/2015/1/Milking-automation-is-gaining-4 popularity-1568767W/.*

[4] "Keeping Food Cyber-Safe". Fponthenet.net. N.p., 2016. Web. 2 Aug. 2016.*http://www.fponthenet.net/article/102963/Keeping-food-cyber-safe.aspx*

[5] Hackett, Robert. "Hilton Is The Latest Hotel Chain To Confirm A Data Breach". Fortune. N.p., 2015. Web.

[6] Two men admit to $10 million hacking spree on Subway sandwich shops. ArsTechnica. from *http://arstechnica.com/security/2012/09/romanians-cop-to-10-million-hacking-spree/.*

[7] Dairy Queen Confirms Breach at 395 Stores — Krebs on Security. (2016). Krebsonsecurity.com., from *http://krebsonsecurity.com/2014/10/dairy-queen-confirms-breach-at-395-stores/* .

[8] P.F. Chang's Breach: 33 Locations Hit. (2016). Bankinfosecurity.com.from *http://www.bankinfosecurity.com/changs-a-7153.*

[9] Cybercrime statistics in India from *http://dazeinfo.com/2015/01/06/cyber-crimes-in-india-growth-2011-2015-study/* .

[10] "Cyber Security Jobs | Requirements And Salaries". Cyber Degrees. N.p., 2016 *http://www.cyberdegrees.org/jobs/*