***Boss, I Think Someone Stole Our Customer Data***

Brett Flayton -> CEO Flayton Electronics

Laurie Benson -> vice president for loss prevention.

They have 32 stores in six states and online stores. His company use payment card industry, PCI standards for data protection. There were no clues for data stealing.

***Comprehensive Approach to Cyber Resilience***

In 2020, most of the companies had gone for work from home for that purpose they collect data from employees that what would be their requirements for working from home. Main concern was that the PCs and other WIFI devices must be secured.

400% companies had faced cyberattacks in 2020 loss of hundreds of thousands of Dollars. In 2020 US lost 1 trillion Dollar. Due to SolarWinds government and fortune 500 companies had suffered from cybercrime. The attack exposed sensitive data for eight months at nearly 18,000 organizations using SolarWinds’ IT management and network monitoring software. Every company needs a proper secured data environment. The first thing is the Data Management, data must travel securely from one place to another in a secured manner and trusted environment in terms of network and data storage.

The questions were:

Where is the data coming from?

How frequently does data change?

Who have access to data? How is data used?

How do you know that data has altered or affected in case of attack? How data can be accessed in case of attack?

Planning and execution need ans to all ques. Cyber resilience can be achieved by identifying how and what sources or devices they used to access data. How data is processed.

**CDO:** Chief Data Officer take decisions about data management during execution and breach situations.

**Data Stewards:** report data to CDO, validate accuracy of data, how data flow from one department to another, ensures how his team is accessing data and are they using right data?

**IT TEAM:** cyber security engineers, how data is going out and coming in the organizations. Gather needs of devices for work from home.

**HR:** bridge between employees and IT department for resource gathering.

**Others:** Data Analyst, Software engineer, utility engineer are assets plus threat to an organization.

**Machine Learning and AI:** need a strong ML and AI algorithm that can detect data breech or attack with in no time.

With the increase in growth of data, the treat to cyberattacks had also increased. If the companies know their threats, then it would be easier to plan against attacks and act accordingly.

***Cyber Attack at University of Calgary***

May 28, 2016 university of Calgary was attacked with cyber breech with pop ups of ransom bitcoins on their screens. Austen (associate Director and infrastructure operation manager) developed an **Emergency Response Team** who ensures integrity of university data assets. Austen’s mind: Where was the problem? Was it a cascading network failure, or was the problem at the server level? And what was it: a propagating virus, a corrupted disk? For some time they thought that the servers was down but then they realized that it was an attack. Heggerud’s (director of ERT) role was to take responsibility for the IT staff during any emergency and to safeguard the incident commander.

Attackers demanded 27 bitcoins in exchange of private key to recover their files in 7 days. Auston’s approach was to handle the situation instead of remediation. His main focus was to preserve data and stop malware from propagating. He disconnected the email server. Dalgetty hired a private consulting firm, who knows how to access dark web as it allows users to do peer to peer communication.

Due to the attack the had almost lost 9k email accounts, and all files were encrypted. So, the put a notice on all gates “not to open PC due to network failure”. IT advisors said that to shut all networks but Dalgetty was concerned about the research work and golden anniversary celebration i.e., reputation. Staff had no access to their data and the news was spreading fast. The decision was made that the ransom word will not be spread outside the CMT room. But the question was how?

Developed a Senior Leadership Team, who will facilitate with their faculty team asked to shift emails to office 365 and use ppr based instructions. After 3 days, they finally started thinking about ransom, so the problem was how to gather the amount because there was not a single policy which will deal with this kind of breech and finance.

On June 1 they gathered a meeting and discussed that the university will be in great financial crises because 27 bitcoin is approx. to $21000. Samsam was the software that targeted private sector encrypt their files, emails etc with the goal of finance. It allows hacker to access domain network using remote network. It uses scanning tool to target their system. And attack at night and encrypt as much as it can. The procedure of buying bitcoin was mentioned in the note.

***Data Privacy in India***

Indian govt had passed a bill named Data Protection Bill which insures the collection, processing, storage, usage, transfer, protection, and disclosure of personal data of Indian residents. They knew their global economy will be $1 trillion in 2022. They passed this bill under EU’s General Data Protection Regulation and restrict their companies to follow that. Don’t act like China. They consider their citizens data as their assets. Many companies had changed their business plan due to this bill. Following are the clauses of Bill:

1. ***Privacy as Fundamental Right:*** don’t misuse citizens data. All digital marketing agencies must use privacy policy to safeguard their data. All the companies who sell their services freely are not allowed to disclose someone’s personal data.
2. ***User Consent:*** take permission at every stage before collecting personal data and let them know the purpose of data collection. As companies send their customer’s data to 3rd party to analyze the data patterns. Companies must know whether, when, and how to obtain user’s permissions.
3. ***Ownership of Data:*** the person who gives his personal data is the owner and have all the rights to take back his data. Companies must ensure that how would they cater this situation. 3rd party involvement must be in mind.
4. ***Three Classes of Data:*** *a) sensitive:* includes: financials, health, sexual orientation, genetics, transgender status, caste, and religious belief*. b) Critical:* government data, eg, national security data, military data. *c) General:* contains rest of the data. Companies should have policies that how to process all types of data. All sensitive and critical data must be stored in India. Critical data cannot be taken out of country.
5. ***Data Sovereignty:*** when the government demands its citizens’ data, in case of foreign attacks and surveillance, digital companies would have to abide and assist the Indian government’s defense policy.
6. ***National Interest:*** government can ask for the data at any time from digital agencies without user consent and the company have to give them. Government cannot take consent from the citizens to process or take their data they have all the rights what to do with their data.
7. ***Verification tag:*** user must be divided into 3 categories i.e., 1) registered + authentic 2) registered + unauthentic 3) not registered. All the users must be verified.
8. ***Compliance and Enforcement:*** in case of data breech for noncompliance agencies penalties would be $700000 or 2% of global revenue. For multinational it would be jail for higher officials.
9. ***Taxing Digital Companies:*** multinational companies don’t pay their taxes. Penalties gave leverage to government to collect taxes from digital companies.
10. ***Other:*** this law is applied to all companies who are collecting data including the company who is collecting data from tractor via sensors.

***Deloitte Cyber Security Role***

**Who are cyber professionals?**

Individuals responsible for protecting an organization’s network, infrastructure and computer systems. Have skills beyond IT including an understanding in business process, vendor management, physical security, threat awareness, and business continuity management.

**Must have Skills:**

1. A strategist to ensure protection of network, infrastructure and computer systems.
2. Must have good communication skill to communicate with team and clients.
3. Technical competency, advancement in skills within time and solve issues immediately.

**Roles and Responsibilities:**

Developing and designing security architecture.

Managing security measures and performance.

Operating regular inspections => security updates.

Conducting audit

Customizing access

Maintain and improving information security.

**Why is there a shortage?**

Toolkits are obtainable with no formal education required to learn. designed to create chaos and opportunities to rob organizations of their assets. Cyber security counter measures are essential because of increasing attacks.

Certificate is required to become professional. No on demand graduates in cyber security. Most organizations face challenges in interpreting the detection or mitigation of cyber security threats.

**What can you do?**

**Re-examine your workforce strategy** => recognize the qualities in IT professional.

Have a **robust support program for new hires** such as mentorships, rotational assignments and shadowing to help new cybersecurity hires to gain visibility and experience.

Build a local **cybersecurity ecosystem** by connecting with government organizations, educational institutions and other groups to explore and generate interest in the cybersecurity field.

Continuous learning and upskilling to defend the attacks.

***Intellectual Property Rights***

Tangible property => bicycle/computer, physical thing that can be protected by laws of theft.

Intangible property/Intellectual property => governed by laws, rights to use, copy, or reveal information about intellectual property. E.g, formula of a drug.

**Types of Intellectual property**

1. **Copy Right**

right to copy, can be anything.

Things that can be protected by copy right: original literary(a table or compilation, a computer program, preparatory design material for a computer program and certain databases), dramatic, musical or artistic.

***Rights of copy right owner***

* Copy from disk to RAM, download page from web.
* The right to issue copies of the work to the public, whether or not they are charged for it.
* Right from translating into other language.
* ***What you can do to copy right work***
* Not make backup of program for which you are not authorized to. 1 copy is allowed.
* Decompile program to remove errors and to gain info.
* Sell a program like you sell a book.

***Database***

The database right subsists in a database ‘if there has been substantial (worthful) investment in obtaining, verifying or presenting the contents of the database’.

It lasts for 15 years and prevents anyone from extracting or reusing all, or a substantial part of, the database without the owner’s permission.

***Copy right Infringement***

Primary infringement takes place whenever any of the exclusive rights of the copyright owner is breached.

Secondary infringement occurs when primary infringement occurs in a business or commercial context. Can lead to heavy fine and even imprisonment. It involves piracy of software for trading or business usage.

***Ownership***

If you work in joint venture then have equal ownership.

If you work for an organization then the owner is employees.

If the author is an independent contractor, he or she will own the copyright unless there is an agreement to the contrary.

The copyright remains the property of the owner, but the *licensees* (the people to whom the software is licensed) acquire certain rights.

1. **Patents**

Temporary right, granted by the state, enabling an inventor to prevent other people from exploiting his invention without his permission. The inventor has to ask for permission and is granted from national patent office.

In order to overcome the fear of copying the government grant patent but after its expiry everyone is free to copy or use. And is only applicable if implemented in hardware.

An invention can only be patented if it:

* is new;
* involves an inventive step;
* is capable of industrial application;
* is not in an area specifically excluded.

Excludes the following:

* Scientific theories: The theory of gravity cannot be patented although a machine that uses it in a novel way could be.
* Mathematical methods: This means, for example, that the methods used for carrying out floating point arithmetic cannot be patented. A machine that uses the ideas can however be patented.
* A literary, dramatic, musical or artistic work or any other aesthetic creation: As we have already seen, these are protected by copyright.
* The presentation of information: Again, this is covered by the law of copyright.
* A scheme, rule or method for performing a mental act, playing a game or doing business, or a program for a computer.

Software can be patented if:

* it is part of a product that is itself eligible to be patented;
* it controls a process that has some physical effect;
* it processes data that arises from the physical world.

Patents encourage investment because:

* a patent is a well-defined asset that allows shareholders and, in particular,
* venture capitalists to be confident that their investment is producing something of value;
* patents ensure that the benefit of research and development accrues to the people who financed it.

1. **Confidential Info:** that should not be passed on.
2. **Trademarks**

identify the product of a particular manufacturer or supplier.

Act makes it an offence to:

* apply an unauthorized registered trade mark (that is, a registered trade mark that you do not own or do not have the owner’s permission to use) to goods;
* sell or offer for sale (or hire), goods or packaging that bear an unauthorized trade mark;
* import or export goods that bear an unauthorized trade mark;
* have in the course of business, goods for sale or hire goods (or packaging) that bear an unauthorized trade mark.

ICANN is ensuring that the same domain name will always lead to the same internet location.

* The potential for conflict between trademarks and domain names is inherent in the two systems.
* Trademarks are registered with public authorities on a national or regional basis. The owner of the trade mark acquires rights over the use of the trade mark in a specific country or region.
* Identical trademarks may be owned by different persons in respect of different categories of product.
* Domain names are usually allocated by a nongovernmental organization and are globally unique; they are normally allocated on a first come, first served basis. This means that if different companies own identical trade marks for different categories of product or for different geographical areas, only one of them can have the trade mark as domain name, and that will be the first to apply.

***Cyber Squatting:*** The inconsistencies between the two different systems of registration has made it possible for people to register, as their own domain names, trademarks belonging to other companies.

***Internet Issues***

Problems due to internet availability:

1. Defamation
2. Pornography
3. Spam

***Internet Service Provider***

* ISP does not initiate transmissions, store information temporarily.
* does not modify the information;
* complies with conditions on access to the information;
* complies with any rules regarding the updating of the information, specified in a manner widely recognized and used by industry;
* does not interfere with the lawful use of technology, widely recognized and used by industry, to obtain data on the use of the information;
* acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.
* it did not know that anything unlawful was going on;
* where a claim for damages is made, it did not know anything that should have led it to think that something unlawful might be going on; or
* when it found out that that something unlawful was going on, it acted expeditiously to remove the information or to prevent access to it, and
* the customer was not acting under the authority or the control of the service provider.

***Criminal Law***

a person, X, commits a criminal offence in country A and then moves to country B.

in principle X can be extradited, that is, arrested and sent back to face trial in A. X cannot be punished in B except some extraterritorial jurisdiction.

***Defamation Act:***

* he was not the author, editor or publisher of the statement complained of,
* he took reasonable care in relation to its publication, and
* he did not know, and had no reason to believe, that what he did caused or
* contributed to the publication of a defamatory statement.

The Internet Content Rating Association (ICRA) is an international, independent organization whose mission, it claims, is: ‘to help parents to protect their children from potentially harmful material on the internet, whilst respecting the content providers’ freedom of expression.’

***Spamming***

* Unsolicited email can only be sent to individuals (as opposed to companies) if they have previously given their consent.
* Sending unsolicited email that conceals the address of the sender or does not provide a valid address to which the recipient can send a request for such mailings to cease is unlawful.
* If an email address has been obtained in the course of the sale of goods or services, the seller may use the address for direct mailings, provided that the recipient is given the opportunity, easily and free of charge, with every message, to request that such mailings cease.

***Computer Misuse***

* unauthorized access to a computer;
* unauthorized access to a computer with intention to commit a serious crime;
* unauthorized modification of the contents of a computer.

The requisite intent is an intent to cause a modification of the contents of any computer and by so doing

* to impair the operation of any computer;
* to prevent or hinder access to any program or data held in any computer; or
* to impair the operation of any such program or the reliability of any such data.

Computer fraud can be stated as a ransomware.

***Intuit India***

Intuit India is a division of Intuit Inc., a financial software company based in the United States. Intuit India is known for its commitment to building a great place to work, and has received numerous awards and recognition for its employee-friendly policies and practices.

One key aspect of Intuit India's approach to building a great place to work is its focus on employee development and growth. The company provides a range of training and development programs to help employees build new skills and advance their careers. This includes training in technical skills such as software development, as well as leadership development programs and opportunities for employees to take on new challenges and stretch their capabilities.

Intuit India also emphasizes the importance of work-life balance and offers a range of benefits and perks to support its employees. This includes flexible work arrangements, such as the option to work from home, as well as a range of health and wellness programs and resources. The company also encourages employees to take time off when needed and offers a generous vacation policy.

In addition to these policies and practices, Intuit India is also known for its strong culture of collaboration and teamwork. The company fosters a sense of community and encourages employees to work together and support one another. This includes hosting regular team-building events and fostering a culture of open communication and transparency.

Intuit India's commitment to building a great place to work has paid off, with the company receiving numerous awards and recognition for its employee-friendly policies and practices. These include being named one of the "Best Companies to Work For" by the Great Place to Work Institute, as well as being recognized as one of the "Top 25 Best Multinational Workplaces in Asia" by the same organization.

Overall, Intuit India's approach to building a great place to work is centered on its commitment to employee development and growth, work-life balance, and teamwork and collaboration. These are key factors that any organization can consider when looking to create a positive and supportive work environment