

Course Name: Cyber Security and Privacy
Professor Name: Prof Saji K Mathew
Department Name: Department of Management Studies
Institute Name: Indian Institute Of Technology Madras, Chennai
Week: 10
Lecture: 30

ABOUT EQUIFAX

- **Founded in:** 1899
- **Business:** Credit Reporting Company
- **Location:** United States
- **Mission:** Responsible for collecting and providing information on income and creditworthiness to organizations and individuals.
- **Company's slogan:** "Powering the world with knowledge"
- **Gross Margin:** Collects consumer and business credit information from banks, analyzes it using proprietary processes and sells the credit analysis giving a **gross of 90%**
- **Customers:** 820 million and 91 million businesses around the world.

BUSINESS SEGMENTS

USIS (U.S Information Services)

- Online information services, mortgage services, mortgage solutions and financial marketing services
- Revenue through sale of consumer and commercial credit reports and scores

Workforce Solutions segment

- Customer data sold to organizations looking for individual employment and income history
- Business services for handling unemployment claims, employment based tax credits, etc.

Global Consumer Solutions Segment

- Providing credit monitoring and identity theft


So, let us see how such a big company faced a data breach.

00:00:32 / 00:41:57

NPTEL

So, a very good afternoon to one and all present here. So, we group two, are here to present about the data breach at Equifax. So, Equifax is basically a credit reporting company and it has all the information that we discussed today, has personal data collected from customers. So, let us see how such a big company faced a data breach. So, brief about the company, the company was founded in 1899. So, the business is basically credit reporting.

It is located in the United States, but serves customers across the world. So, basically like any credit reporting company, it collects customer data which includes their income, information about their income, employment, etc and processes it and also gives results regarding the credit worthiness and credit rating of the person or the institution. So, we have heard about CIBIL, we have CIBIL scores. So, this is very similar to that and the company goes by the slogan that 'Powering the world with knowledge', through the data that it has.



CYBER SECURITY AT EQUIFAX

- Millions invested in Cyber Security measures
- Over 1% of operating revenue spent on cyber security each year between 2014-2017
- Cyber Security expert brought in as the CSO (Chief security officer)
- Who works to modernize Equifax's cyber defenses, rehearsing possible breaches
- Creating 24 hours crisis management squads




Legal/Security Group

- The CLO (Chief Legal officer) supervises the CSO (Chief security officer)
- Security group - 180-190 employees
- They define the "WHAT"
- Security engineering function by providing the ability to configure the software

Technology Group

- Headed by CIO (Chief Information Officer)
- Reported directly to the CEO
- Responsible for deploying the technology that the security team wants in the infrastructure.

Chains of Commands

GTVM

- The Global Threat and Vulnerability Management team
- Tracks threats to the security of the IT systems and notify relevant personnel


VAT

- Vulnerability Assessment Team
- Ran regular scans of IT systems for vulnerabilities

Countermeasures

- Deployed code designed to obstruct the exploitation of ongoing vulnerabilities

Teams



So, we have seen that the company has extensive cyber security measures in place, but still

00:04:50 / 00:41:57

So, the company has a gross margin of about 90 percent and serves about 820 million customers and 91 million businesses. So, the company is divided into three basic business segments. One is the US information services. So, this segment is basically concerned with collecting the customer data. So, it has online information services, mortgage services, mortgage solutions and the revenue that is earned is through the sale of the customer and credit reports of commercials.

The next segment is the workforce solution segment and this segment gets data from the first segment that I mentioned, which is the US information services. So, the customer data which is sold to organization, so they generate individual employment and income history and they also provide other services such as handling unemployment claims, employment tax credits, etc. The third segment is the global consumer solution segment which provides credit monitoring and identity threat protection. Moving on. So, we know that this company is like an information extensive company and it has personal data of consumers.

So, it is very crucial for them to have a cyber security system in place. So, the company has invested millions of dollars in cyber security measures right from 2005 and over 1 percent of their operating revenue is spent solely on cyber security measures, each year from 2014 to 2017. Apart from this, they also had a cyber security expert as the CSO, the chief security officer and he basically works to modernize the cyber security practices in the company such as the cyber defenses and they also have a special squad. So, they have a crisis management squad which they keep running, in rehearsing in case of any breaches. So, with respect to the chain of command, they basically have two groups.

One is the legal or the security group and the other is the technology group. The first group that is the security group is headed by the chief legal officer and he supervises the CSO, who is the chief security officer and under him there are about 180 to 190 employees and the other group is headed by the CIO, that is the chief information officer and he directly reports to the CEO. So, what is the relation between these two groups? So, security group basically defines what has to be done and the technology group is concerned with deploying the technology that the security team asks for and the security group also has a security engineering function and they provide ability to configure the software. So, apart from this, they have multiple teams which are specifically working for cyber security. So, one is the GTVM which is the global threat and vulnerability management team.

So, this team is concerned with tracking the threats in the IT system and they have monthly meetings where they are notified with respect to any possible cyber threat that is there. The second team is VAT which is the vulnerability assessment team and they basically run scans with respect to the vulnerability in the IT system. The third is the countermeasures. So, this team is with respect to implementation. So, they deploy the code designed to obstruct the exploitation with the ongoing vulnerabilities which is identified by the GTVM and the VAT team.

So, we have seen that the company has extensive cyber security measures in place, but still they were exposed to a huge data breach. So, let us see what are the vulnerabilities that they had. Moving on, Subisha will continue. So, we have till now seen how much they have invested for cyber security and how many teams they have deployed for cyber security measures. But still we have come across a breach in 2017, which was one of the world's most massive breach that we have seen.

So, I have a question for you. If credit bureau's customer data is leaked, what is the privacy risk as an individual you can face or what are the impact as an individual you can face? Like what can be the motive behind the attack? There can be various uses of a personal data that a hacker can use it for. It can be just to put someone into a ransom kind of situation or it could be used for tracking purposes, it could be used, if it is health related data, health expenses or credit related expenses. It can be used to bring certain kinds of threats from a financial standpoint, from an insurance standpoint, from the banking services standpoint. So, it is a variety of ways in which the personal data can be used.

You are absolutely right. So, you have... It can actually be used for, like identity theft.

So, if a person has a good credit score, another person can use the same details to take a loan in the other person's name and then not repay the loan, commit loan fraud. So, the

original person will now get the indebted. You are right. And apart from the reasons mentioned, it can also be directed for targeted ads because almost all your financial data would be leaked if such a breach happens because when you go to Experian or Equifax or TransUnion civil page, you go and enter all the data. For example, in Indian context, you would be entering Aadhaar, passport, driving license, everything.

So, it poses such a grave risk. So, basically what happened is they had so many security issues and vulnerabilities. For example, it didn't start in 2017. It started from 2013 when many hackers could access the credit report data from Equifax. Then 2015, there was a technical error which was caused by some software modifications which publicly exposed so many consumer information.

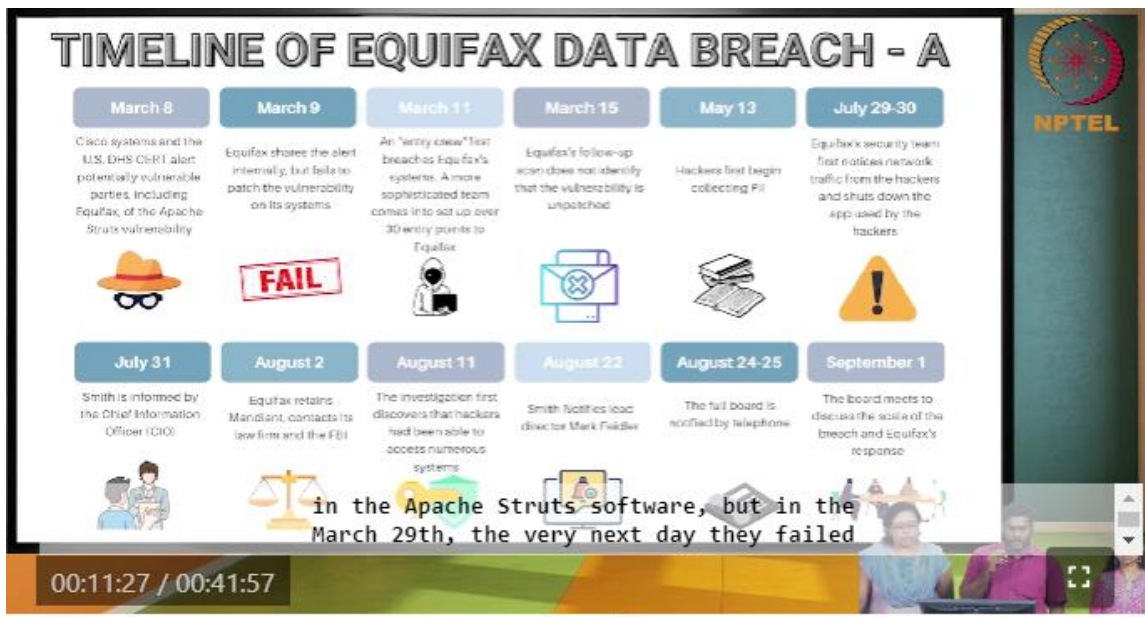
And in 2016, almost like 4,31,000 employees salary and tax data was publicly exposed and this was even brought out by independent researchers. So, in 2017, before this breach happened, there was something called Equifax work solutions in which the employee tax documents were being freely downloaded by the attackers. So, all this security vulnerability was not brought into notice. It was known to them. Because there was a cyber security firm called Mandiant which warned Equifax about its, how its systems were unpatched and misconfigured.

And it had also hired Deloitte, to credit, to conduct a security audit which also said about the several issues about its unpatched systems. Even cyber security firm called Cyence also quantified the probability of Equifax encountering a breach which was about 50 percent. Another group called FICO that is Fair Isaac group also analyzed the corporate cyber risk to be 550 out of 3 which was a range from 300 to 850. And BigSight Technologies, it gave F grade, that is the worst for application security and D grade for software patching. So, MSCI's research team also gave 0 for privacy and basically lower, almost lowest rating of triple C for privacy and data security.

So, we will go into what caused the data breach of 2017. So, there was, this was caused by Apache Struts vulnerability and basically Apache Struts is an open source software which was used to build Java applications. It was widely used across banks and financial institutions and it was access and Apache, they got to know that there was a publicly available exploit in their system. So, once they got to know, they warned everybody who were using this application. So, in this exploit, the attackers could add their own code to the web pages, even disable firewalls, install malwares and even access servers etc.

So, about patching the vulnerability, since this was a grave issue and so many, so many companies were using using this Apache Struts vulnerability, CERT of US department had alerted all these vulnerable parties and one of them was Equifax. So, immediately

this GVTM team also got the message, but most of the monthly meetings were not even attended by the senior officials or even the cyber security members of the Equifax itself. So, they did not take this seriously and even the countermeasures team at Equifax delayed their steps so much as we can see in this diagram, that is March 7th Apache Struts is you know, telling about this vulnerability and it is having 5 months to take, it is taking 5 months to take corrective action by Equifax because that is when they come to know about this breach. So, now we will look at the timeline of the data breach of from when it started. So, it started on the March 8th.



So, that is when the other Cisco systems and other parties, they alert that there is a vulnerability in the Apache Struts software, but in the March 29th, the very next day they failed to patch the vulnerability on it is a system. And then in March 11th, that is when the hackers they gain access to their systems and then again when they get to know then the Equifax they failed to identify the vulnerability which is unpatched. So, that lead to an major data leak and the hackers were able to collect the personally identified, personally identifiable information of all the customer data. And then on July 31st, that is when the chief information officer, he was informed about the data breach which is currently happened. And before that, prior to that when they were able to shut down this like, they were able to track the IP addresses from where the traffic was coming, but they were not able to they blocked one, but they were not able to block the multiple thing.

So, they went to shut down the system and then they contact their law firm and the FBI and they ask them to conduct an investigation into these issues. That is when they know that they have been able to access the number of systems within the Equifax. Then the Smith, he notified all the team members through their phone call and they would ask them

for an board meeting. So, when it comes then, that is when they come to an list, they say that it is about 143 million consumers have been affected. So, all their personal data have been stolen and it has been in the hands of the hackers and then they announce it publicly.

And that is when the Equifax, after these issues the CSO and the CIO, both resigned and even the CEO also resigns after that. And then after, apart from this 143 million data, there is an additional 2.5 million data also has been stolen, which they did not confirm it at the earlier stage. And then the Smith, the CEO, he testifies before on the US government committees and the last, the what about 10 million in the data driver license and is stolen and about 7 million, about 7 lakh UK customers are being affected. And they had a contract with Equifax, the IRs so it got suspended due to these issues.

So, now we will see at the breach, like what was the actual and how it has happened. So, the hackers, that they created when they gained access to an Apache, through the Apache Struts app software, they created an 30 backdoors using the web shells which nobody, the Equifax failed to notice it. So, by doing so, they gained an increasing difficulty of finding for the Equifax to identify where the breach or the door was open to it. And SSL security certificate, that is the, it needs to be renewed between every 12 to 39 months, but the Equifax they had always the expired, it was expired across the network. So, that is why they were easily able to gain the access.

And then the ACIS reactivated, that is they blocked the IP address which caused the traffic, but again and they gave the portal was open, the patch was unable to fix it. So, again the hackers from the China they were able to gain access and that is when they went on to shut down for the 11 days. And then the web, so he is the CEO of the Equifax. So, he did not make clear that the PIE data has been breached at the earlier, it was around in the month of May or earlier, like 2 years prior to that. And then that is when the Equifax and the mandatory investigation, it happens.

So, they get to know that they have accessed the data table containing the large amount of the consumer data. So, what kind of the information has been stolen? It is the names, social security numbers, birth dates, addresses, email id, driver license, credit card number, passport number, your tax identification number and the credit card dispute documents. So, now we will see the sources of the vulnerability inside the Equifax which lead to this data breach. First one is the internal controls and the patch management process. The roles and the responsibilities in the patch management committee, the policy were ambiguous.

So, the business owner, the software owner and the system owner were not uncertain, about their roles and what each has to do in this kind of activities. And in the 2015 audit,

so which was conducted by the Deloitte and the other professionals, so it was said that around 8500 unpatched vulnerabilities were there and until 2017 they were not able, it was not a resolved or neither the systems were patched. And due to this lack of systems, that is the comprehensive inventory of the IT systems which lead to it. So, Payne, he is a CSO and the secretary were unaware that the ACS ran the Apache Struts. So, they were not aware about their internal systems and the process which was happening at the Equifax.

And in 2015 the patching was taken as an reactive measure rather than an proactive. So, only when a system is gone down, so that is when they update the systems and make it, like usable. So, it is more like, what is only on the request basis. So, it was not taken as an a priority of measures. And the employees, they gave the reasons for the weakness at the Equifax.

So, one is the technology systems were not well integrated. So, it has difficulty in updating. So, they were, since there are lot of the systems, around 8500 unpatched systems, they were finding it difficult to find the right patch, for the vulnerabilities for that. And then they antiquated systems. So, update themselves, so which lead to an operational risk.

For example, we will see that our Windows, it gets updated like, it goes for an automatic update and your work has to be like shut down for some time until your system is back on the screen. And they also, they did not have a personnel necessary to implement the technologies and a process to meet the internal security goals. So, that again, it leads to the accountability gap in the organization structure. So in, until 2005, the reporting structure was that a CSO reports to the CIO and to the CEO. But due to an interpersonal conflict at the, at the duration of 2005, the CSO and the CIO were independently reporting to the CEO.

And then there was no clear communication between both the teams. Then the IT and the security team were, there was no communication. So, it was an ineffective and inconsistent communication between them. And that is when the Payne, he testified that there are key vulnerabilities, but they have been not resolved until and also they did not take any action to like, unload the Apache Struts software. And the only interaction between the IT and the security were during the monthly meetings and the senior leadership meeting.

SOURCES OF VULNERABILITY INSIDE EQUIFAX

Internal Controls and the Patch Management Process

- Roles and responsibilities in Patch management policy were "ambiguous"
- 2016 Audit - 8500 unpatched vulnerabilities, unresolved till 2017
- Lack of comprehensive inventory of IT assets, Payne and security personnel were unaware that ACIS ran Apache Struts
- 2016, Patching was reactive rather than proactive, lead to lag in the installation of critical patches, no verification
- Reasons for weakness:
 - Technology systems were not well integrated/difficult in updating
 - Antiquated systems: update themselves Operational risk
 - did not have personnel necessary to implement the technologies and process to meet internal security goals


"Accountability Gap" in the Organizational Structure

- 2006, reporting structure CSO-CIO-CEO interpersonal conflict
- IT and Security were siloed, inconsistent and ineffective communication
- Payne testified key vulnerabilities implicated in data breach, but not resolved in time to fend off Apache struts hacks
- Monthly meetings and senior leadership meetings failed - "Clear lines of accountability for developing IT security policies and executing the policies"
- Security concerns were presented by CLO, had no experience or training in information security

Technological Barriers to Effective Oversight

- Failed to identify and address potentially malicious activity on servers, ACIS 1970s
- ACIS system lacked file integrity Monitoring (FIM) process - Scan for unauthorized, suspicious alteration in IT systems and configurations
- Web servers retained log files for 30 days, NIST recommends for at least 3 months, detected targeted attack after 98 days (avg)
- Did not have process for ensuring SSL certificated were up-to-date throughout the organization
- Jan 2017, internal audit addressed the concerns of SSLV devices missing certificates, but the problem went unaddressed - 324 expired SSL certificates, 79 in critical business

First one is the internal controls and the patch management process.

00:15:16 / 00:41:57


But those failed because they failed to identify their clear lines of accountability for developing the IT policies and executing the policies. And the security concerns were presented by the CLO that is the chief legal officer and none of the CSO or neither the CIO, he has the, like authority to present all those. And the CLO, he had neither experience nor the training in terms of the cyber security or the information security. And the third barrier that is the technological barrier to an effective oversight. So, when the breach happened they failed to identify and address the potentially malicious activity on the servers.

So, they had an old, which is about 1970s that is the only security they had, ACIS which was in 1970s and they had not updated their systems to the current 2000s or 2015. So, they lacked the, the ACIS system and lacked the file integrity monitoring process that is for, it cannot scan for an unauthorized access and neither it can scan for the foreign suspicious events which has happened in the systems and the configurations. And they did not according to the NIST documents, the Equifax should have an log data for about 3 months, but they used to clear their log data within 30 days and they were not able to track or analyze any of their breaches which could have happened in the past and so that they could have taken a priority measures. And neither they did not have a process for an ensuring an SSL certificate were upto date throughout the organization. So, as we have mentioned, so it was an outdated system and in January 2017, the internal audit addressed that the concerns of the SSL devices were missing, but the problem went unaddressed and then that is when there were 324 expired SSL certificates are on the organization and then 79 in the critical business domain.

So, all of these certificates were grouped together and the business segmentation was

not there within the organization. So, all were put into the same domain and that is when the hackers got access to the systems. Now, we will look at the breach announcement and the response. So, till now we have seen how many security vulnerabilities they had before the breach. So, after the breach did they tackle correctly? That is what we are going to see.

So, the PR announcement was that, was came in September 2017, but the breach started in March itself. So, they announced the data breach publicly that 143 million American data, people's data had been exposed and they also put out a website to help the customers determine if they were actually attacked or not and they engaged many cyber security firms like Mandiant to assess the risk. So, basically the steps they had taken is, they had credit file monitoring, Equifax credit lock, identity theft insurance, then also dark web scanning for one year. All these were provided free for one year after which, but they these customers had to sign a controversial clause saying that they will not sue Equifax for their data breach. So, their impact on stock prices was that it fell from 143 dollars to 93 dollars in a week which declined by 35 percent and other impacts were, as we have already seen like driver license data, customer data etc and passport details were compromised.

And in this the, there were some missteps, actually this controversial clause angered the customers because they could not sue the company. Then they started charging customer for credit freezes, then all these identity threat protection was only for one year after which they had to start paying and the breach time was announced very delayed. And even the Equifax twitter handle, it directed the customers to a fake website with somebody else had started. So, even they were not very, you know did not take safety measures regarding that. So, basically the, they had 11 member board of directors with 9.

3 year tenure and this was the only credit reporting company which had a separate technology committee consisting of 5 members, even then this breach happened. This technology company reviewed the company's technology investments and including all these policies related to information security etc. So, having seen how severe the impact has been, let us see what the fallout was. So, as mentioned earlier there was a steep decline in the stock price of about 35 percent and the key executives- the CSO, the CIO and the CEO as well as the chairman, they resigned from the company and lost their jobs. So, there was also a consideration of clawing back of the compensation of two of the employees and one of whose was the CEO himself.

So, they also had plans to bring in a new director, McGregor. So, he was a person who was experienced in cyber security, information security and had extensive experience. So, as we have seen in many other cases earlier, one of the key consequences of a data

breach is the legal implication. So, there were lawsuits and government inquiries by the New York state attorneys as well as the Federal Trade Commission and all of them conducted formal investigation which led to bad image of the company and apart from this, they also had a act which was enacted, Freedom from Equifax Exploitation Act. So, the purpose of this was to enhance the fraud alert procedures and providing free access to credit freezes.

So, Subisha mentioned what credit freezes was. So, apart from this, there was a investment group called Change to Win and so this was basically an investment advisor and shareholder activism group and they provided six proposals to Equifax. So, they said that if these proposals were not followed, then there would not be a re-election of the new director, McGregor as I mentioned. So, what were the six proposals? So, the first one was improving the governance and holding executives accountable. So, we have seen how important governance and compliance is and the executives did not have proper communication and this was one of the main reasons for the breach. The second was removal of the chairman of audit and technology committees.

So, though they had a technology committee, they did not perform their duties diligently. The next one was permanently separating the CEO and the chairman positions and last one was considering legal settlements when you are creating the compensation for executives. So, basically this committee, they threatened that if these six proposals were not followed then they would not go about electing the new director. So, coming to the disclosure. So, as she mentioned earlier, there was a huge gap about six weeks between the discovery of the breach and the disclosure of the breach to the public.

So, actually US did not have a proper regulation in place for disclosure. So, one said that it was 45 days and few others said, did not have any guidelines at all. So, what they did was, there was a proposal of bill where they had a unified 30 day time frame for alerting the consumers in case a data breach happened. And they also, the New York attorney also held Equifax very strict disclosure requirements. So, they had to alert within 72 hours to the state regulators in case a breach has happened.

So, now let us see what we learnt from this case which is one of the largest data breaches after Enron. So, moving on to Subisha. So, moving on to the last part. So, how big is the Equifax hack, that you can see from this diagram. So, it had compromised almost 143 million records, while in 2017 the adult population in US was 254 million.

So, almost half. So, and they had severe impact, that is profit fell by 27 percent, 90 million dollars breach related cost, 240 customer lawsuits and separate investigation by many organizations. So, was Equifax alone while tackling this breach? Did other

company also face similar breaches? In 2017 alone, 3785 corporate companies had fallen as a victim of cyber attack in the US and Cisco found that 55 percent of the surveyed companies had a data breach in 2017. So, it was not Equifax alone and many large cap corporations lost almost 500 billion in the market capitalization for major cyber attacks that happened on an average in this year. So, it is a question for you to ponder whether Equifax was just negligent or just plain unlucky. Based on the details you pointed out, I guess it was pure negligence from the Equifax too because as there were many security lapses, like they were using outdated services and lots of even their Twitter handle was not, it was directing to a different site.

So, I guess it was a negligence from such a big corporation and which is handling such a sensitive data. You are absolutely correct. No technology system is 100 percent secure that we know for sure, but there are certain basic measures which each company needs to take to the extent possible to safeguard its data and especially if it is a company like Equifax, which is dealing with highly confidential data, it needs to go the extra mile. But there were gaps, like patches in the system were not put in place, security certificates had expired, which could not detect the data packets which the hackers was taking out of the system. From a governance and from the organizational structure standpoint, there were various red flags that security issues were not even reaching the senior management, the CEO had no clue because the reporting structure was such that the legal officer did not have a background in that and the security came under the legal officer.

In 2013, there were many exits, the CSO had exited. There were a lot of exits in the security department which was again a red flag, but no one really looked into it. So, there were a series of issues which the organization did not address which would be classified as negligence. Those measures should have been taken, but even then the attack would have been there, but various measures on this front segmenting of database etc could have helped minimize the impact. You are absolutely right. There were so many red flags, like CERT had pointed out what the vulnerability was and they had to patch it within 48 hours, but they had not taken any impact, any measure and also the meetings who had attended, who had not attended, even they did not have a log of that.

Yeah, but I have a different view. See as you pointed out, Equifax was not the only company which went through cyber attack. The point is we are doing this analysis post hoc. Having all this happened, we have a lot of information, but when a company is on its business, keep in mind that Equifax is not a technology company. Its main business is data. Actually customers are the suppliers and also customers, in a business like this.

So customers bring the data and customers are given information. So that is their business and you also see that they had several acquisitions and when you acquire companies, you

acquire their technology which may not well integrate with your system and some of them may be outdated. So these are all problems that commonly organizations face and it is not that you will upgrade all systems in one go and make it updated. So you all work with this reality that there will be old and new systems and upgradation may take time and that may be the case with other organizations too and that is how business function. So and they had an organizational structure where there was a well defined CSO's role and then there was a CIO role and they have put in place some structure.

Of course it was not perfectly functioning. So why do you find so much fault with Equifax just because the case got documented and you have a lot of information, but that is all post hoc. You can always find fault with the government after some decision goes wrong, but when they are taking the decision, we have nothing to say. So I think that I would just side with Equifax, well they were unlucky. But they could have updated the systems or at least for smaller batches, so they could have reduced their risk. Apart from this, there was one important reason which was regulations and after this breach, each one had different regulations which were followed amongst credit reporting agencies as well.

So after this breach, they had unified credit reporting regulations which were imposed. So I think the regulations which are not in place cost was one of the reasons why so many breaches happened at that time. Also to address Sir's point, Equifax is not an ordinary organization. It is obviously going to be a very valuable target for all attackers because it hosts half the population of USA's information. Because it has likelihood of being attacked is much higher, therefore the responsibility of defending it from such attacks is also higher.

They should have been more proactive in that sense. Cyber attacks happen to one organization almost every day, but since it is not an ordinary organization, it should have been more proactive in that sense. They cannot escape on the fact that it is a statistical possibility that they will get attacked. And also before the breach itself, many firms had pointed out that there are many security vulnerabilities and they had not taken so many initiatives on that as well. We can see from 2013 to 2016, before the major attack of 2017, they did face a lot of attacks based on the timeline. But still they were negligent from their standpoint, I believe, in order to not update their regulations as well as the cyber security system.

And being a credit bureau organization, I believe that they should have taken such necessary standards. Even if they were late to the party, they should have been a forefront in having such systems in their hands, I believe. Should we have been more like, it should be classified as a critical infrastructure, like what we have in India, CIA designated organization has to have high level of cyber security protection. So this is one of those organizations. And also maybe out of the 3,785 organizations, like none of them might

not have this amount of data.

Maybe that business operations might have been different. So considering that maybe the Equifax should have been more addressed, they should have addressed it at an earlier stage, when the patch went unnoticed. So any other questions? Should we adapt this is based on trust and faith of the customers? And in fact, once they came to know that the breaches happened, then also they were not showing any kind of, you know, sincerity or sincerity in their approach, delaying disclosure and all and again charging fees for their freezing and all those things. So we cannot say that they are unlucky.

They were in fact to gross negligence after the incident also. Yes. So okay, assuming that you win and you say that, well, they could have conducted their business better. So if overall, if you look at it, well, there are many failures, but whom would you attribute this to? Where lies the major problem? You see that the case talks about issues right from regulation at the country level to board level to CEO level and to managers level, okay, employees level. But where would you actually find a major issue? One or two things which really caused this problem. Majorly the governance issues becomes so clear. So they were, when they restructured it, they were not clearly mentioned about who the roles and responsibilities were not clearly mentioned.

So they appointed a CLO, so who is supposed to give the reports of information security, but he is an, neither he had any experience nor training in the information security. So somebody listening to an inexperienced person, they might not take an immediate actions. So they might just consider it as like an incident or like okay, it has happened, so it can be handled later. The effect, the critical of the issue might have been not addressed very well within the organization. Okay, so there is a structure in place which is two command centers for IT and security and it is coordinated, of course at the CEO level and that is how they structured it, but it was not functioning effectively.

But a board may not be getting into the day to day running of the organization. But if you have to find fault with the board, did board have any information that they should have acted on? I think in 2015 audit when they conducted, so they told that the system, the eight key facts, all the systems went unpatched. So even after addressing, after two years when the breach happened, still the patch was not fixed, neither there was not any measures taken to update it. Okay. So that audit report was widely shared within the, like board members. And also this vulnerability was very grievous that the US Department of Homeland Security intervened and told all the vulnerable parties to immediately address it.

So even after that, there was delay and among the employees of the Equifax, who were

had not updated the patch, there was not even a counter checking whether they had updated or not. And in March this happened, in April meeting, April GTVM meeting they did not even address this issue again. They did not ensure if the March breach was addressed or not. So there was no proper implementation even though they had invested so much for all these measures. So this case has become a case of corporate governance basically, right, or enterprise risk management.

So as you say there was inputs from the government and also independent agencies which rated the cyber security level of Equifax as very low, right, ACCC for cyber security. And that is a publicly available document. So what is the role of independent directors? Basically in a board meeting, our role is to ask questions to the management. Why is the security rating so low? That is, of course a governance issue.

Governance, you need to monitor how systems are performing and ask questions. So there is at least two things that I see as very striking as governance failure. One is that the directors or the board did not even react, proactive, they did not even react to the scores, the security scores that came after studying their security systems. And also the management was not functioning effectively. So there is obviously a problem there which is related to governance, corporate governance issue. So you can see for large organizations like this, cyber security should be a important thing for the board to monitor and be aware of.

How BIG is the Equifax Hack?

Equifax 2017
143 million records
Note: "Criminals gained access to sensitive files in the company's system from mid-May to July by exploiting a weak point in website software."
- New York Times

254 million people
adult population
of the US

Heartland Payment Systems
134 million records

Target
100 million records

TJX Companies
64 million records

Home Depot
54 million records

CONCLUSION & TAKEAWAYS

- Profits fell by 27 pc year on year
- 90mn\$ breach related costs
- 240 customer lawsuits
- Separate investigations by FTC, CFPB, SEC, British and Canadian regulators

Was Equifax Alone?

- 2017- 3785 Corporate victims of cyber attack in the US
- Cisco found 55% of the surveyed corporate had a data breach in 2017
- Large cap corporations lost 498mn\$ in market capitalization for major cyber attack on average

Was Equifax negligent or just plain unlucky?

00:27:01 / 00:41:57

That is one thing this case or this incident has taught corporations. And therefore when you deploy technology, the failure of technology can actually lead to massive loss and

loss of reputation in the market. And not only financial loss, to make up for the, of course you see how the stock prices fell. So it is huge impact and that is basically a governance issue which ultimately if you analyze this case. So if the structures are not in place, so then the system will respond accordingly.

So that is a very important point. Is there anything else? Alright, so we will conclude this case. We see that cyber security is not a technical, it is not just a technical issue but it is a corporate governance issue as well. So that is the way it escalates or you can see it becomes for large organizations. And it also touches on need for regulation. For example in how many days it should have been reported.

So if it is reported early as an individual, I can stop my cards. If my credit card information has gone out, I can say, well I can inform the bank, I can take proactive action. But if it is not informed to me, it is loss for me. So there should be a clear regulation from the government. So that is what we see how different is GDPR in terms of making this as part of regulation, making it mandatory for all countries in the EU.