INDEX

Boss I think someone stole our costumer data:

Intro:

- The CEO of Flayton Electronics, Brett Flayton, receives a memo from the head of security about a potential data breach at the company.
- The vice president for loss prevention, Laurie Benson, informed Brett that Flayton Electronics has been identified as a common point of purchase for a large number of fraudulent credit card transactions by Union Century Bank.
- Brett is concerned about the potential consequences of a data breach and asks Laurie for more information. Laurie explains that it is possible that Flayton Electronics is the source of the data leak.

New Territory:

- Flayton Electronics, a fictional electronics company, is facing a potential data breach after a routine analysis by Union Century Bank identified fraudulent credit card charges made at Flayton's on almost 15% of compromised accounts.
- The company's CEO, Brett Flayton, and the VP of Loss Prevention, Laurie, are discussing the potential implications and actions to take in response to the situation.
- They consider the possibility of customer notification, the potential financial exposure for the company, and the various ways in which the data could have been compromised.
- They also discuss the importance of data protection and the role of senior executives in ensuring the security of company data.

Limited Defenses:

- It is revealed that the company is only compliant with about 75% of the Payment Card Industry (PCI) requirements for data protection, and it is not clear how the breach occurred.
- Brett knew that PCI compliance, which was mandated by all the major credit card companies, required regular scans by an outside auditor to ensure that a company’s systems were working—with stiff penalties for failure.
- “They don’t scan us every day,” Sergei demurred. “Compliance really is up to us, to me, in the end.”

Core Values at Risk:

- As Brett Flayton contemplates the potential consequences of a data breach at the company, he reflects on the decisions he has made in recent years to aggressively grow the company and the potential impact on its infrastructure and systems.
- He wonders if he has pushed for too much growth too quickly, potentially leaving the company vulnerable and underinvesting in its systems.
- He also considers the potential impact on the company's reputation and its core values, as represented by the photographs of satisfied customers on the walls of the stores.

Into the breach:

- Flayton Electronics has discovered a disabled firewall in their wireless inventory-control system, which could have allowed internal company data to be broadcast.

- The human resources director has identified five former employees who were involved with the system and notes that two of them were terminated for misconduct.
- The communications director has presented the company with three options for handling the situation: holding a press conference, informing customers by letter, or doing nothing until law enforcement is ready to go public.
- The outside counsel warns that going public first could lead to lawsuits from customers, banks, and investors, and notes that some states require immediate disclosure while others do not.

How should the Flayton Electronics team respond to the crisis?

4 commentators offer expert advice:

by James E. Lee:

- For Flayton Electronics, moving swiftly in the face of crisis will be essential
- Beyond fix ing the firm's weaknesses in data security, CEO Brett Flayton must develop a brand-restoration strategy. The company should, as ChoicePoint did, notify the affected customers rapidly, set up toll-free information hotlines, and offer credit-monitoring services.
- Flayton's will also have to address the influence of blogs, viral videos, and other social media. Such user-generated content, unfiltered by traditional journalists and accessible by anyone using an online search engine, is often a mode of recruiting lawsuit plaintiffs and airing personal grievances.

by Bill Boni:

- Businesses should have a high-level official, such as a director or a vice president of information protection, who serves not merely as a manager but as a senior champion in this area.
- One useful strategy is to identify the data that might be involved— and their value. This mandate builds appropriate safeguards right into the projects themselves.
- Being fully PCI compliant is, of course, a vital first line of defence against data theft, and my best guess is that a third of companies meet that standard.
- You need people on hand with the digital expertise to match wits with tech-savvy cyber criminals and to understand the systems they're targeting
- You can assemble an internal team of lawyers, accountants, and experienced digital-forensic investigators from law enforcement or defense agencies—or use external sources such as law firms, public accounting firms, and consultancies with digital specialization

by John Philip Coghlan:

- A study by Javelin Strategy & Research, 78% of consumers said they'd be unlikely to continue shopping at a store once they had learned of a data breach there.
- So our harried CEO has no better option than disclosure. If he doesn't speak out, he is not allowing his customers the best means of protecting themselves
- The electronics firm has built its reputation on honesty. So Flayton Electronics must communicate— right now—with its customers

- Research from Bain & Company also offers some hope: Customers who receive adequate compensation after making a complaint are actually more loyal than are those without complaints.

by Jay Foley:

- The companies that get sued are not those that are first to go public about a data breach but those that do so poorly.
- Another misconception of the management team at Flayton's is that they should consider notifying customers themselves
- If Flayton's rushes into a public announcement, the bad guys have the chance to disappear, only to resurface elsewhere. Nothing positive will have been achieved with that result.
- The company's first action should be to reduce the risk for future thefts by closing any data-transaction loopholes that this incident has brought to light.

********** THE END **********

Apple vs. Samsung: The $2 Billion Case - 1

- Apple Inc. claimed that Samsung Electronics had copied some of its patents.
- These patents covered a variety of touchscreen interfaces, including the following: “pinch-to-zoom”, “double-tap-to-zoom”, “rubber-band” and “snap-back”
- Apple filed a lawsuit that claimed that they had suffered a revenue loss of 2 billion US dollars.
- To defend this figure, Apple hired a team of researchers, led by John Hauser Professor of Marketing at MIT’s school of management, who conducted a discrete conjoint analysis to prove that Apple Inc did indeed a suffer revenue loss of $2 billion because Samsung copied its patents.
- Samsung of course did not agree with the method of study and pointed out flaws/biasedness in it.

Conjoint Analysis: Conjoint analysis is a statistical method used in market research to understand how consumers value different features of a product or service. It involves presenting consumers with a series of product profiles that vary in terms of certain attributes, such as price, brand, or features, and asking them to choose their preferred option. By analyzing the choices made by consumers, researchers can estimate the relative importance of each attribute and calculate the overall value that consumers place on the product or service.

The Conjoint Study in the Apple-Samsung Case:

- The expert witnesses brought in by Apple developed two separates, but similar, online surveys—one for smartphones and another for tablets. Each one included a discrete choice conjoint model, comprised of six features.
- **If the primary issue was related to touchscreen capabilities, why did the conjoint analysis include four other features (not including price)?** Because by including other features, the products were more fully formed and hence more realistic. Further, the other features were helpful in masking the true focus of the study and thus providing reliable results
- **How did Apple choose these seven features chosen from a much larger subset?** These were among the features highlighted on Samsung’s own website, and were also those used in other technology websites for smartphone and tablet comparisons.
- Apple narrowed down the levels of the features that were both most relevant to consumers and were at issue in the case. Each of the six features were described by four levels. For example, the levels of the Storage feature were: 8 GB, 16 GB, 32 GB, and 64 GB.
- conjoint choice tasks also include a **“none”** option that allows consumers to indicate their lack of interest in any of the alternatives presented to them in that specific question. Based on the proportion of respondents who choose this “none” option, researchers can estimate primary demand for the product
- After running through standard quality checks, the smartphone (tablet) study had a final tally of 455 (415) respondents

The Results: Adding up the “Partworths”:

- Primary results from conjoint studies are ***partworth*s**—essentially, attractiveness scores

for each level of each feature The more attractive a level is (say 32 GB compared to 16 GB), the higher the partworth of that level.

- In other words, partworths provide a common and convenient metric for evaluating the total value of a product
- In conjoint analysis, a very useful tool called a ***market simulator*** is often used. Its input is the partworth scores of individual respondents
- the difference in price between the two products provides an estimate of the premium that can be charged for the superior touchscreen capability. Such an analysis allows calculation of consumers' willingness to pay a price premium for certain features
- Unwilling to accept Apple's calculations, Samsung hired its own experts. Not surprisingly, these experts proceeded to point out flaws in the design of the conjoint conducted by Apple.

********** THE END **********

Apple vs Samsung: The 2$ Billion Case - 2

Samsungs Rebuttal

- Samsungs teams primary issue with Apple's design was it omitted many features that are important in the decision of buying a smartphone/tablet.
- These included brand and battery life.
- They argued that omitting such features put an emphasis on less important features such as the superior touchscreen capability.
- Wharton Professor David Reibstein, was hired by the Samsung team.
- He wrote in his report, "You're trying to predict what it is people will buy, and if you just focus on smaller aspects and a couple of major factors, you're going to miss what would drive sales and why people would buy your products."
- Reibstein contended that it was like conducting a study of cars and asking people what type of cup-holder they would prefer rather than asking about the brand.[Chris Smith, "Samsung: Apple's Patented Software Features Are as Trivial as Cup Holders in a Car," Yahoo! News, April 21, 2014, http://news.yahoo.com/samsung-apple-patented-software-features-trivialcup-holders-144151542.html.]
- Another expert witness, Tulin Erdem of the Stern School of Business at New York University, conducted an eye-tracking study to identify which features consumers were looking at when choosing a smartphone or a tablet.
- Based on this study, she argued that Apple's expert witness study had flaws: "You are elevating artificially the importance, the value of these things. They are not even in the radar screen of consumers. These are very granular . . . and they wouldn't drive demand." [2 Mikey Campbell, "Samsung Experts Say Apple's Patented Features Not Valuable in Trial," Apple Insider, April 18, 2014, http://appleinsider.com/articles/14/04/19/samsung-experts-say-apples-patentedfeatures-not-valuable-in-trial. Ina Fried, "Samsung Expert Says Apple's Damage Calculation Methods All Wrong," Recode, April 18, 2014, http://recode.net/2014/04/18/samsung-expert-says-apples-damagecalculation-methods-all-wrong/.]
- Samsung's expert witnesses also argued that focusing the study only on the Samsung brand (i.e., not including Apple or other competitive brands) was another important flaw in the study's design.

Key Learning Points from the use of Conjoint Analysis

- Conjoint analysis is a robust and widely used approach, commonly used to measure consumers' willingness to pay for product features.
- This approach is particularly useful in new product design, in order to select which new features to develop.
- The approach has been applied across a variety of product categories, including: cars, hotels, credit cards, pharmaceutical drugs, and cameras.
- Conjoint analysis has also been frequently used in litigation cases involving billions of dollars in claimed damages.
- However, there are several issues to consider when using conjoint analysis:

Survey Design

- Often products have many features, and deciding what to include, and hence what to leave out, is not easy.
- In the case of smartphones or tablets the number of features can easily exceed a hundred.
- Since survey respondents have only limited resources in terms of time and attention, it is not practical to include every feature of a product in a conjoint study.
- However, the way a conjoint study is designed can frame the product in the eyes of the consumer, potentially over- or underestimating the importance of certain features.
- Typically an effort is made to include major features such as brand and price to ensure that the basic building blocks of the decision are accounted for in the design.
- Apple's study design did not include brand (and hence a competitive context).
- Their argument was that the primary objective of their study was to measure the value of added features, which should not depend on which brand the feature is added to.
- Thus, since primary demand was not being estimated and the interest was only in the trade-off between the specific features in the litigation and price, it was not necessary to include brand as a feature in the design.
- Samsung's argument was that without the major features, the study's design was flawed— and it ultimately overestimated the importance of the features being tested.

Competitive Environment

- Conjoint studies often assume that the market is static in terms of competitive reaction, which is not always the case.
- For example, if Samsung were to introduce a product with different touchscreen capabilities, both Apple and Samsung would most likely adjust their products and prices leading to a different market outcome.
- Therefore, when possible, conjoint simulators should capture the market environment and competitive reactions.
- Capturing competitive reactions in the study might complicate the design, thereby compromising the data quality.
- Thus, there is a trade-off involved in the design of the conjoint itself.

Study Participants

- The type of respondents included in the study will have an impact on the results, based on their level of exposure to the products in the market.
- For example, Apple's study included only Samsung users, while Samsung contended that the study should have been more broad-based.

********** THE END **********

Mount Everest Diasater

1. The 1996 Mount Everest disaster was a tragic event in which eight climbers lost their lives while attempting to summit the mountain.
2. Many of the climbers were inexperienced and did not have the necessary skills or knowledge to safely navigate the mountain.
3. The lack of knowledge and experience contributed to the breakdown of learning in the teams.
4. Poor decisions and ineffective communication were among the problems that resulted from the breakdown of learning.
5. The climbers were unable to provide the necessary guidance and support to ensure the safety of their teammates.
6. The 1996 Mount Everest disaster highlights the importance of effective communication, leadership, and learning in teams.
7. A breakdown in these areas can have serious consequences.
8. Ongoing learning and development is important for individuals and organizations.
9. The disaster serves as a cautionary tale about the importance of these factors.
10. Poor decision-making was a major factor in the disaster.
11. Many of the climbers made poor decisions that ultimately led to the tragedy.
12. Poor communication was also a contributing factor.
13. The climbers were unable to effectively communicate with each other, leading to confusion and misunderstandings.
14. Inadequate leadership played a role in the disaster as well.
15. The climbers were inexperienced and did not have the necessary skills or knowledge to effectively lead their teams.
16. This lack of leadership contributed to the breakdown of learning in the teams.
17. The 1996 Mount Everest disaster demonstrates the importance of strong leadership in ensuring the safety and success of a team.
18. Effective communication is also critical for the success of a team.
19. In the case of the 1996 Mount Everest disaster, the lack of effective communication contributed to the breakdown of learning in the teams.
20. Ongoing learning and development is essential for individuals and organizations.
21. It is important for individuals to constantly seek out new knowledge and skills in order to improve their performance and contribute to the success of their teams.

22. Organizations also have a responsibility to provide their employees with the necessary training and support to ensure their success.
23. The 1996 Mount Everest disaster serves as a reminder of the importance of ongoing learning and development.
24. The tragedy could have been prevented if the climbers had possessed the necessary skills and knowledge to safely navigate the mountain.
25. The breakdown of learning in the teams was a major factor in the disaster.
26. It is essential for individuals and organizations to prioritize ongoing learning and development in order to prevent similar tragedies from occurring in the future.

Overall, the 1996 Mount Everest disaster highlights the importance of effective communication, leadership, and learning in teams, and the consequences that can result from a breakdown in these areas.

Organizational disaster:

- Organizational disaster research aims to understand the factors that lead to breakdowns in organizations and the mechanisms required for recovery. There are several streams of research on disasters, each focusing on different levels of analysis.
- One stream focuses on how individuals and teams conceive, deliberate, and act upon organizational problems, such as groupthink and the failure to respond to small setbacks.
- Another stream focuses on systemic factors, such as the degree of interconnectedness or 'coupling' in a system and organizational culture, that lead to disaster.
- A third stream seeks to integrate multiple levels of analysis, looking at how cognitive, systemic, and institutional factors work together to create a disaster.
- An emerging theme in disaster studies is the importance of leadership in preventing and responding to disasters. Research has also highlighted the role of communication, training, and contingency planning in preventing and responding to disasters.

Learning and organizational disaster:

1. Research has begun to assess how organizations can learn from mistakes, adapt to changing technologies, and surface errors before they escalate into disasters.
2. Factors that lead to learning breakdowns in teams may be different from those that enhance learning.
3. Team learning is essential for effective performance, particularly in complex tasks with a wide range of contingencies and potential responses.
4. The 1996 Mt Everest disaster will be used as a case study to explore learning in teams through a qualitative analysis.

Methods:

The 1996 Mt Everest climbing disaster, in which 15 climbers died and several others were seriously injured, served as the data for a study on learning and its breakdown in teams. The study focuses on three expedition teams and the deaths of eight climbers as an example of organizational disaster.

Data collection:

1. Data for the study on learning and its breakdown in teams was drawn from multiple public sources, including published accounts, photographs, charts, and Internet filings by expedition teams.
2. Data collection began immediately after the 1996 Mt Everest disaster and continued until the preparation of the manuscript.
3. Efforts were made to obtain accounts from as many participants as possible, including post hoc data from the Internet and documents produced by survivors in the aftermath of the events.

Analytic strategy:

1. A timeline of events was created from a review of public accounts, and this timeline was turned into a narrative by identifying and organizing the sequence of events, clarifying important attributes of the actors, creating the context, establishing an evaluative framework, and setting the narrative voice.
2. Mohr's process approach to theory construction was used to refine the data, synthesize relevant constructs, and generalize the events. This approach involves identifying the focal unit of analysis, precursors (discreet events or processes), motivators (forces that initiate the precursors), probabilistic processes (forces that bring the precursors together), and outcome (impact of the combination of precursors on the focal unit).
3. The analysis was enhanced by the personal experience of the researcher, who was in the Everest region in the aftermath of the disaster and participated in conversations with individuals associated with the mountain-climbing community.
4. The combination of these strategies aimed to achieve medium accuracy, medium generality, and low simplicity in the trade-offs inherent in qualitative research.

The final assault:

1. The New Zealand (NZ) and American (US) teams were two of the 30 expeditions attempting to summit Mt Everest in 1996.
2. The NZ team consisted of 15 members, and the US team consisted of 12 members.
3. Both teams reached the highest camp (Camp IV) on May 9 and set out for the summit in the early morning of May 10.
4. The teams had to secure safety ropes along the Southeast Ridge Balcony between 27,200 and 28,000 feet, creating a bottleneck that slowed their progress.
5. The teams were not equipped with radios to communicate within or between teams, and they had established turnaround times ranging from noon to 2 p.m. for when to abandon their efforts for the summit and begin descent.

Traffic jam at the summit:

1. A bottleneck occurred at the Hillary Step, a difficult section of the climb just below the summit, at around 11 a.m. to 12 noon.
2. Between 1.12 and 1.25 p.m., eight members of the NZ and US teams reached the summit, followed by more members between 2.00 and 2.15 p.m. and around 3 p.m.
3. US guide Fischer and NZ guide Hall reached the summit with clients an hour and a half after the agreed upon turnaround time, and a member of a fourth team from South Africa reached the top of the mountain at 5 p.m., nearly four hours after the agreed upon turnaround time.

The descent:

- The 1996 Mt Everest disaster occurred during the final stages of a climbing expedition, with 15 deaths and several serious injuries.
- The disaster was caused by a combination of factors, including an impending snowstorm, exhaustion due to climbing for longer than the 18 hours for which climbers were equipped, and the lack of supplemental oxygen and other support.
- The disaster also resulted from bottlenecks and delays caused by issues with fixed safety ropes, as well as the late arrival of some team members at the summit. The disaster highlights the importance of team coordination and effective decision-making in preventing organizational breakdowns.

The huddle:

- There were three expedition teams attempting to climb Mt. Everest in 1996: the New Zealand team, the American team, and the Taiwanese team.
- The teams experienced bottlenecks and delays while climbing, which caused some members to abandon their summit attempt.
- Despite this, several members of the NZ and US teams reached the summit between 1.12 and 3.00 p.m. on May 10.
- A snowstorm slowed the descent and caused difficulties for the climbers, who were not equipped for such conditions.
- Several team members, including the leaders of the NZ and US teams, became lost in the storm and went missing.
- Some members of the teams were left behind on the mountain and believed to be dead, while others made it back to their camps.

Rescue Attempts:

- The disaster involved three expedition teams: the New Zealand (NZ) team, led by Rob Hall; the American (US) team, led by Scott Fischer; and a Taiwanese team.
- Bottlenecks and a lack of fixed safety ropes caused delays on the climb, and a storm slowed the descent.

- Several climbers ran out of supplemental oxygen and became exhausted, leading to panic and contemplation of death.
- Rescue efforts were complicated by the extreme altitude and bad weather.
- Eight climbers died in total, including three guides and two Sherpa guides.
- Several other climbers were injured, including Gau and Weathers who both suffered amputations.

Analysis:

- The Mt Everest disaster can be used as a source of data for analyzing team process due to its classification as a disaster "incident" and meeting the criteria for a critical event worthy of research
- The Mt Everest disaster has symbolic importance beyond the local climbing community and has been used to illustrate various organizational phenomena such as leadership, strategy, and ethical decision-making
- The Mt Everest disaster fits criteria for developing general theory from particular experiences and provides data on an understudied level of analysis (teams in organizational disaster) and type of team (task forces, expeditions, short-term project teams)
- The Mt Everest disaster can be studied as an example of a team goal that requires the ability to shift course based on new information and address multiple goals and changing circumstances
- Team learning, as proposed by Mills, is central to team success when confronted with a complex and challenging task and includes processes such as selecting and screening information, drawing conclusions from extant experience, and distinguishing important information from the irrelevant and insignificant.

Discussion:

- This study looks at the breakdown of team learning in the face of a changing environment and provides a process theory of team breakdown, identifying key variables that led to the breakdown
- The study highlights the importance of team-level learning for organizational learning and focuses on the process factors associated with the breakdown of team learning
- The study suggests that face-saving behaviours, such as psychological safety, may be an interesting area for future research in relation to organizational disaster
- The study has particular significance for learning in short-term project teams that may prioritize performance over learning
- The study suggests that the changing nature of the mountain-climbing industry may have contributed to the Mt Everest disaster and highlights the need for multiple-goal organizations to rely on multiple agendas with alternative pathways in order to adapt to changing circumstances.

- This study found a close relationship between learning and leadership and showed how leadership can sometimes inhibit team learning
- The study suggests that the temptation of goal achievement can overtake a leader's ability to consider alternative courses of action and that narrowly defined goals and the rewards of achieving them can lead to organizational breakdowns when combined with restrictive learning and complex problems
- The study calls for further research on a comprehensive process model of learning in short-term project teams in the face of complex tasks, including a new logic of goal-setting those accounts for unintended consequences and the impact of learning procedures on team functioning
- The study also suggests that future research should focus on how leaders tempt teams into taking risky actions and how narrowly defined team purpose can limit learning
- The Mt Everest disaster provides a unique example of the breakdown of learning in teams and highlights the limits of rational goal-setting, the need for more research on short-term project teams, and the role of leaders in limiting team member learning. It also illustrates how muddled decision-making during high-altitude mountain climbing may provide insight into how traditional teams respond to and recover from organizational disasters.

********** THE END **********

Apple v Samsung (Opinion) before Bryson, Prost & O'Malley, Circuit Judges

Bryson, Circuit Judge's Observation:

- The appeal was made from the denial of a preliminary injunction.
- Although it presented substantial evidence of laws, the jurisdiction of issuing preliminary injunction belongs to district courts.
- Which is why it was difficult to overturn the decision.
- W.r.t two patents in the appeal , the appellant did not prove an abuse of discretion
- So the Denial of preliminary injunctive relief was reaffirmed.
- W.r.t another patent, district court committed legal error in an imp aspect.
- Therefore that portion of the courts order and remand for further proceedings will be vacated.

A:

- Apple, Inc., is the owner of several design and utility patents pertaining to smartphones and tablet computers.
- The iPhone embodies U.S. Design Patent Nos. D593,087 ("the D '087 patent") and D618,677 ("the D' 677 patent").
- Those patents issued on May 26, 2009, and June 29, 2010, respectively
- Apple also owns U.S. Design Patent No. D504,889 ("the D'889 patent"), which is directed to the design of a tablet computer.

The design of Patents:

- Both patents claim a minimalist design for a rectangular smartphone consisting of a large rectangular display occupying most of the phone's front face.
- The corners of the phone are rounded.
- The D '087 patent claims a bezel surrounding the perimeter of the phone's front face and extending from the front of the phone partway down the phone's side.
- The D'677 patent does not claim a bezel but instead shows a black, highly polished, reflective surface over the entire front face of the phone.
- The D'677 patent disclaims the sides and back of the device.
- The D'889 patent depicts a rectangular tablet with a polished reflective surface extending to the edge of the front side of the device.
- The front face of the patented design has rounded corners, and a thin bezel surrounds the front surface along its perimeter.
- The front surface has no ornamentation, buttons, speaker slots, holes, or raised surfaces.
- Apple claims that its iPad tablet computer embodies the design of the D'889 patent.

B:

- Apple filed suit against Samsung on April 15, 2011, alleging, inter alia, infringement of the D '677 patent.
- Two months later, Apple amended its complaint and asserted that Samsung was also infringing the D'087 and D' 889 patents.
- Apple claimed Samsung's Galaxy S 4G & Infuse 4G infringed the D'087 and the D'677 patents.
- The phones were released on February 23, 2011, and May 15, 2011, respectively.
- Apple also alleged that Samsung's Galaxy Tab 10.1 tablet infringed the D'889 patent.
- The tablet was released in June 2011.
- On July 1, 2011, Apple moved for a preliminary injunction to block the importation into and sale within the United States of the accused Samsung devices.
- The district court denied Apple's motion with respect to each of the accused devices and all four asserted patents.
- The court noted that four factors must be considered in addressing a motion for a preliminary injunction:
    1. whether the movant is likely to succeed on the merits.
    2. whether the movant is likely to suffer irreparable harm in the absence of an injunction.
    3. whether the balance of the equities favors the movant.
    4. d whether the public interest would be served by the grant of injunctive relief.
- The claims based on the D '087 and D'889 patents were denied relief.
- This was on the grounds that Apple had failed to show a likelihood of success on the merits.
- The claims based on D '677 patent were also denied relief.
- This was on the grounds that Apple had failed to show that it would likely suffer irreparable harm from Samsung's continuing infringement while the case was pending before the district court.

C:

- The court first examined the D'087 patent.
- It concluded that the patented design did not cover functional features.
- However, substantial questions were raised about the patent's validity.
- Therefore, Apple had failed to show that it was likely to succeed on the merits.
- The court held that the front view was likely anticipated by Japanese Patent No. 1,241,638 ("the '638 patent").
- The court found the D'087 design to be substantially similar to the '638 patent.
- This was due to it having "similar edges and rounded corners, a bezel, a similarly shaped speaker, and similar proportions of screen and border.".
- The '638 patent, the court found, "discloses an overall simple, minimalist design."
- The court rejected Apple's argument that the arched profile of the front of the '638 design differed from the flat profile of the D'087 patent.
- This was in light of the fact that the sides and back of the phone were disclaimed in the D '087 patent.
- So the court held that it was improper to consider anything other than the front views of the two designs.
- Apple failed to establish the first factor needed for a preliminary injunction.

- Therefore the court did not reach the other three preliminary injunction factors for the D'087 patent.

D:

- The court then addressed the D'677 patent.
- The court again looked to the '638 patent as a primary reference.
- But concluded that the '638 design was sufficiently different from the D'677 patent that it would not have been obvious to a designer to adopt a "flat, black, translucent front screen."
- The court therefore concluded that Samsung had not raised a substantial question regarding the validity of the D'677 patent.
- As to infringement, the court found that both the Galaxy S 4G and the Infuse 4G phones had an overall design that an ordinary observer would likely find substantially the same as the claimed D'677 design and that those phones were likely to infringe.

- Despite these findings, the district court denied Apple's request for a preliminary injunction.
- This was due to Apple failing to show that it was likely to suffer irreparable harm from the importation and sale of Samsung's infringing smartphones while the case was pending in the district court.
- Apple made two arguments in support of its claim of irreparable harm.
- First, it argued that Samsung's sales eroded Apple's design and brand distinctiveness, resulting in a loss of goodwill.
- Second, it argued that Samsung's sales took sales away from Apple and resulted in Apple's losing market share.
- Apple argued that those losses would be difficult to quantify.
- And that monetary damages thus would not be adequate to compensate it for the injuries caused by Samsung's infringement.
- The district court rejected both contentions.

- The court was unpersuaded by Apple's first argument because "Apple has not articulated a theory as to how erosion of 'design distinctiveness' leads to irreparable harm in this case."
- The court also rejected Apple's related assertion that Samsung's sales of infringing phones diluted Apple's brand value.
- Because "even assuming that brand dilution could arise from design patent infringement, Apple has not met its burden to provide evidence that such brand dilution is likely to occur in this case."
- The court held that "[w]ithout more evidence ... Apple has not demonstrated that brand dilution is likely to occur."

- With respect to the claim of market share loss, the court noted that Apple and Samsung were directly competing "for new consumers [who] are looking to make first-time smartphone purchases [and] thus the potential for harm from infringing conduct is strong."
- The court added that the initial decision regarding which product to buy can have long-term effects on items such as downstream purchases.
- The court also observed that there may be "network compatibility" effects that stem from a particular purchasing decision.
- They argued that a purchaser of one phone system may be reluctant to switch to a competing phone for fear of incompatibility with previous digital purchases.

- The court concluded that the economic effect of such losses of customers and future downstream purchases would be difficult to calculate and could support a finding of irreparable harm.

- The district court nonetheless declined to issue an injunction with respect to the D'677 patent because it concluded that Apple had failed to establish a "nexus between Apple's harm of lost customers and loss in market share and Samsung's allegedly infringing conduct."
- The court found that despite Apple's evidence that "product design generally is at least one factor.
- And for some people may be the primary factor, influencing a person's decision to purchase a smartphone.
- " other evidence indicated that the "driver in consumer demand may be the novelty of the product, and not necessarily the design"
- and that "smartphone buyers are motivated to purchase products for a whole host of reasons."
- **That evidence included exhibits showing that only a small percentage of all smartphone purchasers bought the device because of its design.**
- The court concluded that the evidence was "even more ambiguous in light of the fact that Apple's patents do not claim the entire article of manufacture."
- The court concluded that the absence of a nexus between the claimed design and the loss of market share, coupled with Apple's delay in seeking an injunction, undercut Apple's claim of irreparable harm.
- The Court observed that Apple claimed that Samsung was copying its designs since 2007, but failed to file suit till 2011.
- The court rejected Apple's argument that its delay should be excused on the ground that the parties were engaged in negotiations, because the negotiations only covered part of the period of delay.
- Therefore the court concluded that "Apple has not met its burden of establishing that Samsung's allegedly infringing products will likely cause Apple irreparable harm."

- The court held that the balance of hardships favored Samsung
- The court found that in light of the presence of other smartphone manufacturers in the market, it was unclear that an injunction against Samsung's devices would significantly benefit Apple, even though it would substantially injure Samsung.
- Finally, the court found the public interest factor to be neutral.
- Based on its four factor analysis, the court refused to enjoin sales of the Galaxy S 4G and Infuse 4G smartphones.

E:

- The court conducted a similar irreparable harm analysis for the D'889 patent and the Samsung Galaxy Tab 10.1 tablet.
- With respect to the tablet patent and product, however, the court found that Apple had shown a likelihood of irreparable harm
- The court reached that conclusion for several reasons.

- First, the tablet market appeared to be dominated by only two manufacturers, Apple and Samsung, who together controlled a substantial share of the market.
- The evidence suggested that Apple's market share decreased in accordance with the increase in Samsung's market share after the introduction of the Galaxy Tab.
- Secondly, the court concluded that design mattered more to consumers in tablets than in smartphones.
- Finally, the court found that delay was not an issue in the case of the request for preliminary relief against Samsung's tablet.

- The court nonetheless concluded that a preliminary injunction should be denied.
- As there were substantial questions about the validity of the D'889 patent, and therefore Apple was unable to show that it would likely succeed on the merits.
- The court also performed its obviousness analysis.
- The court characterized the visual impression of the patented design as a "broad, simple design that gives the overall visual impression of a rectangular shape with four evenly rounded corners, a flat glass-like surface without any ornamentation[,] a rim surrounding the front surface, ... [a] flat [back] panel that rounds up near the edges[, and an] overall design [that] creates a thin form factor."
- According to the court, the design created basically the same visual impression as a prototype tablet developed in 1994 by Roger Fidler.
- For the flat glass screen, the court turned to the 2002 Hewlett–Packard Compaq Tablet TC1000, which "contains a flat glass screen that covers the top surface of the tablet and a thin rim that surrounds the front face of the device."

- The court found that the combination of Fidler and the TC1000 would likely render the D'889 patent obvious.
- And therefore rejected Apple's secondary consideration evidence.
- The court concluded that Apple's secondary consideration evidence failed to overcome the substantial questions of invalidity and that Apple had not established that it is "likely to succeed at trial against Samsung's challenge to the validity of the D'889 patent."
- With respect to the issue of infringement, the court found that the design of the Galaxy Tab 10.1 would appear substantially the same as the D'889 patent in the eyes of an ordinary observer.
- The court thus denied Apple's request for injunctive relief with respect to the D'889 patent.

********** THE END **********

Ensighten Case

- Josh Manion: CEO of Ensighten.
- It was December 2010, and Manion had moved his software company from Chicago to Silicon Valley
- The company first announced its product in September, and it only had 5 customers
- After 5 months of work, Manion was close to landing Global Media, Incorporated (GMI)
- GMI was a Fortune 50 company, with leading media properties all over the world.
- Manion described the situation as: “As a new venture, with little money, trying to establish not just our company but the space itself, it is tempting to do anything to get a deal done. But, I can’t set the precedent of giving away the store. There are terms in our licensing contract we need to fight for. . . . Establishing that precedent will save us a lot of fights down the road. By the same token, I don’t want to lose this deal.”
- Quinn, a partner and intellectual property specialist with the law firm Larkin Hoffman in Minneapolis, offered his view: “At the end of the day, you have to figure out what you need to have and fight for it. Your success is a matter not just of your legal strategy but also of the fundamental value proposition of your business . . . how critical is the product or service you are selling and how badly does the customer want it . . . . That leverage can buy you a lot.”

The Problem

- Manion observed that Companies struggled with tracking consumer behavior on a website.
- The earliest solutions were built around “weblogs,” a detailed map of all the activity in the browser . . . but tracking and analyzing that data was terribly cumbersome.
- The follow-up to that approach, introduced in about 2002, was page tagging.
- Basically, you put an invisible piece of code on every web page, and when that page is opened, it sends a message to an analytical application that is measuring the desired characteristic.
- So, for instance, if you want to track where a customer comes from, you put a tag on the landing page, and when that page opens, the tag sends a piece of data to the analytical application that is tracking the origin of the customer.
- The same principle applies to the links people click on, the amount of time they spend on a page, and where they go when they leave.

- In practice, there were many analytical applications that required the use of tags to collect the data that could, in turn, be analyzed and acted upon. They included:
- Advertising tools that tracked the effectiveness of ad campaigns, traffic from affiliates, and retargeting or redirection of traffic.
- Analytics packages that tracked where customers came from, how long they stayed, what links they clicked on, if and how much they bought, and where they went. Popular tools in this space were provided by companies like Omniture, Google Analytics, and IBM’s Coremetrics.
- Testing and optimization tools that tested different versions of a web page against each other.
- Voice-of-customer packages that tracked surveys and other consumer feedback and input.

- Manion explained how this increasing trend toward the collection and analysis of web data had created the opportunity for Ensighten:
- A big company could have literally hundreds of sites (or domains) for various product divisions, geographies, and customer types.
- Then, each site could have tens or even hundreds of thousands of pages. . . .
- Imagine what the full set of products and web pages looks like for companies such as Sony or 3M.
- And then, each page could have from 10 to 50 separate tags . . . a tag for each type of data or activity that the company wants to track . . . where did the customer come to that page from, how long they stayed, what they did when they were there, where they went next, what did they buy etc.

Ensighten's Solution

- Manion and his coders developed a simple solution to the problem.
- "Once you had our system up and running, you could do a piece of work like this in literally minutes without sacrificing the richness and complexity of data or analytical output. It was a big idea."
- We announced our product and our first five customers in September 2010.
- We were half a dozen developers and three salespeople.
- It took about $1 million in capital to reach this point
- Despite moving to Silicon Valley, they decided to not raise VC funding.
- Ensightens Product lived in the "cloud."
- The company had contracts with the largest providers of server capacity in the world with numerous clusters of servers running globally.
- This was a critical piece of the application, because every client site reached out to Ensighten's hosted server to know what tags to serve to each visitor to the client's site.
- Ensighten's success in attracting some large clients resulted in this activity quickly building to many billions of requests each month.
- Ensighten priced its services based on the number of websites or client domains and the amount of traffic on those domains.
- A typical early deal was approximately $200,000 in annual licensing fees and a $25,000 setup and installation charge.
- Ensighten could usually configure the service for a client in about a week, and the client could be up and running on the service after that.
- One of the biggest obstacles Ensighten had to overcome was the fact that we needed to convince very large enterprises to rely on us as a mission-critical platform in their infrastructure

Developing a Template Contract

- Working with our law firm in Chicago, they developed a template for their basic software license.
- With our first three clients this worked fine, as we did not run into a major level of legal/procurement review.
- These early agreements helped us to learn what customers were going to push back on and what terms were truly important for us to insist on having; but these early negotiations with

clients focused mainly on the business terms and for the most part did not include legal counsel on either side.

- There were some terms that we stood completely fast on . . .
- Especially ones related to our intellectual property. . . .
- We weren't going to share that with anyone.
- I was also reluctant to provide any levels of indemnification that could put us out of business.
- I was also wary of terms that could put us in the position of having to give a client money back, since we intended to leverage this capital to accelerate our growth.
- On other issues, I would try to accommodate requested changes if they seemed reasonable, especially if it seemed likely that future clients were going to ask for it.
- Hired Jim Quinn, who was an expert at technical details.
- Quinn offered his perspective on the general legal arena in which Ensighten's agreement was grounded:
- In the old days, there was a pretty clear licensed software model.
- A license is a revocable, non transferable, nonexclusive right to use.
- It made sense for Microsoft to license Word or Oracle to license its database software because the license does not confer ownership, and therefore, it allows the licensor to impose a much more restrictive set of terms on the client.
- In an outright sale, ownership confers with it the right to do whatever you please with what you have purchased.
- Software licensors restrict the ability of the licensee with respect to the purpose to which the product is put, for example, the ability to copy or sell services based on the software to others.
- Now, with the guts of the software sitting in the cloud, it is a bit different.
- The customer doesn't even get a copy of the software. . . . They get a right to access the software that is sitting in the cloud.
- Essentially, by paying a fee, the customer gets the right to use the functionality of an application without ever putting the actual software on their computer.
- Of course, the customer still gets a little piece of software that sits on their hardware and serves as a connector, so technically, it may make sense to license that, but the bulk of the functionality takes place in the cloud.

GMI

- GMI was a $70 billion company with leading media properties located all over the world.
- It naturally used many tag-based solutions and wanted extensive tracking of where its customers came from, what they did on the site, the advertising they were served, how effective that advertising was in driving follow-on behavior, and a host of other factors.
- Negotiations with GMI had begun in October 2010, and Manion and the business team at GMI had reached substantial agreement on the business terms by early November.
- Based on this, Manion had provided GMI with Ensighten's standard licensing agreement, the agreement he'd refined based on the first several deals, and an agreement Quinn had blessed after getting involved with the company.
- After a few weeks, Manion had received a redline version with GMI's requested changes to the agreement.
- While he dearly wanted to land GMI, there were certain changes he was wary of making. He decided it was time to depart from his usual approach.

- He called Quinn and involved him in the negotiations: “It is a big deal for us, and while I am comfortable having pushed this 80% of the way, I don’t want to make a mistake at this point.”
- Quinn offered his thoughts:
- GMI is going the typical route here, using outside counsel. For a company of their size, a $200,000 deal isn’t big enough to pull the general counsel and his staff away from core legal issues. So, their outside attorney is probably working within a fairly fixed set of parameters his client has given him . . . “we never compromise on X, Y, and Z, and see how much you can get us on A, B, and C.” The problem is, we don’t yet know which issues are which . . . so, we need to push a little on all sides to see where the box really is. And, the hope is that the issues they will compromise on are the ones we need some movement on. We’ll see.
- Manion reflected on his agenda for the call:
- One issue we need to resolve is around data security.
- Customers are naturally concerned with this, but the fact is, we don’t intentionally keep any data.
- Every page of traffic passes through our cloud-based servers, and we apply the appropriate set of tags to each page as it moves through, but that is all we do. All of the customer’s data—as well as the output generated by the tags—goes to the company or its analytics vendors. We keep nothing.
- We’ve come a long way and I do believe this is a big idea with tremendous upside. But, we have to make progress one deal at a time, and this is a big one. Quinn and I have to come up with a workable approach.
- I know that the attorneys always feel like they need to stake out aggressive positions so we have somewhere to compromise, but I do want to be sure we don’t scare them away with any positions we take. On the other hand, there are some things we just can’t live with in this deal, let alone allow them to become part of agreements with other clients

Question from Assignment

GMI, being a huge company (worth $70 billion), a fortune 50 company, wanted the terms of agreement to be as inclined to them as possible. So they added an abundance of clauses that were in favor of them, and unfavorable to Ensighten.

Some of the clauses included:

1. **Multiple Failures:** “*In the event the Customer is entitled to availability credits more than twice during any four consecutive month period, the customer may terminate this agreement and receive an immediate refund of all amounts paid to Ensighten in connection with this Agreement.”*
2. **Interoperability:** *“The customer and contractors engaged by the Customer have the right to review, access, modify, configure and reconfigure materials,items information, content and technology provided by Ensighten under this Agreement…”*
3. **Termination by Customer:** *“In addition to its termination rights specified elsewhere in this Agreement, the Customer shall have the right to immediately terminate this Agreement in the event Ensighten fails to perform any of its obligations, or is in violation of any of the terms*

and conditions of this Agreement, and Ensighten does not cure such failure within thirty (30) days after the Customer has provided notice of such failure."

This scenario teaches us that in any contract negotiation, both parties ideally want the terms to be as much as in their favor as possible. We have to probe a little and identify what clauses the other party is flexible on and try to get ours accepted by them.

According to James P. Quinn, GMI's attorney was working on a fixed set of parameters given, *"we never compromise on X, Y, and Z, and see how much you can get us on A, B, and C."* He further went on to say: *"The problem is, we don't yet know which issues are which . . . so, we need to push a little on all sides to see where the box really is. And, the hope is that the issues they will compromise on are the ones we need some movement on. We'll see"[* Lena G. , Michael J. , 2013 , Ensighten, Harvard Business School]

********** THE END **********

Cyber Attack at Univeristy of Calgary

University Of Calgary

- University of Calgary (U of C) is a public research institution in Alberta, Canada
- Established as a separate, autonomous university in 1966
- Approximately 30,000 undergraduate and graduate students and 5,000 academic and non-academic staff, 5 campuses, including one in Doha, Qatar
- 14 faculties offering over 250 academic programs
- Eyes High strategy aims to make U of C a top-5 research institution in Canada
- Ranked 8th in Canada by Center for World University Rankings in 2016
- One of four comprehensive academic and research universities in Alberta and one of 15 large research universities with medical schools in Canada (U15 Group)
- Board of governors responsible for overseeing management and operation of university
- Hosted 2016 Congress of the Humanities and Social Sciences in spring 2016
- Campus opened to 1,200 displaced wildfire victims in spring 2016
- Spring session classes cancelled to accommodate conference and displaced individuals.

EMERGENCY RESPONSE TEAM RESPONSE TO INFRASTRUCTURE FAILURES

- Austen is the head of the emergency response team (ERT) at the University of Calgary (U of C)
- ERT activated on May 28 when U of C's system was breached by ransomware
- IT leadership and Catherine Heggerud, director of customer engagement and experience, called in to help respond to the breach
- Linda Dalgetty, vice-president of finance and services; Janet Stein, director of risk management and insurance; and Rae Ann Aldridge, associate vice-president of risk, also called in
- ERT and supporting IT team assembled by 8:00 a.m.
- Ransom note discovered at 2:00 a.m. on May 28
- Ransom note demanded payment of 27 bitcoin with deadline of 7 days or private key would be permanently deleted
- Fortunately, Janet Stein had signed a cyber-liability insurance policy with access to an independent breach coach just a few days before the breach
- Austen's priority was containment to preserve data and stop malware from propagating, not remediation
- Decision made to disconnect network to contain malware but this would affect the entire university's operation
- Option of turning off active directory servers, which power email system, considered but ultimately rejected
- Decision made to isolate affected servers and restore services from backups
- Austen and team worked throughout the weekend to restore services
- Campus community informed of the breach on May 30
- Payment of ransom not considered as it was not clear if private key would be provided after payment
- Investigation into the cause of the breach launched

- Emergency response plan activated and revised in light of the breach.

CRISIS MANAGEMENT TEAM EVALUATION AND HANDLING OF THE BREACH

- Linda Dalgetty is the leader of the IT crisis team at the University of Calgary (U of C)
- Team includes breach coach and consultant from a major consulting firm, and cybersecurity team
- Malware highly sophisticated and caused servers to go down, files to be encrypted, and email to come to a halt
- Communication on campus a challenge with over 9,000 email addresses lost
- Immediate solution was to use posters on entrance doors asking faculty and staff not to turn on computers due to network failure
- Executive leadership crisis management team (CMT) held first meeting at noon
- Dalgetty informed Bonnie DuPont, chair of the board of governors, of the emerging crisis
- IT crisis team made recommendations to CMT, CMT took decisions to board of governors
- Decision made to not go public with the breach
- Rumour mill turned quickly and story leaked to the public
- U of C website landing page and Twitter account used for some information sharing
- Specific communication channels set up through UC Emergency Mobile app to allow emergency operations groups to communicate with leadership team
- Senior leadership team (SLT) composed of 56 campus leaders met on Tuesday and Thursday of the first week to receive updates and ask questions
- SLT also responsible for sharing information with the rest of the community
- Campus community informed of a network breach on May 30 through email and social media
- Campus community asked to not turn on their computers until further notice
- Campus community also asked to be patient and understanding as the IT crisis team worked to restore services
- Campus community reassured that no personal or financial information had been compromised
- Update emails sent to campus community daily
- Decision made to hire a third-party cybersecurity firm to investigate the cause of the breach
- U of C decided to not pay the ransom
- Cybersecurity firm worked with IT crisis team to restore services
- Campus community informed of restoration of services through email and social media
- Review of emergency response plan launched in light of the breach.

MALWARE, RANSOMWARE, AND CYBERCRIME

- SamSam known to attack healthcare, government, and education sectors, but more public organizations disclose attacks than private organizations
- Over half of SamSam's victims are from the private sector
- SamSam targets more than just user documents, also encrypting configuration and data files required to run applications and email clients
- SamSam believed to be designed and launched for financial gain, targeting critical infrastructure systems

- SamSam exploits vulnerabilities in systems to penetrate networks using a remote desktop protocol and steals domain administrator credentials
- Hackers use stolen credentials to take control of a server and use it as a command center to map out the network
- Hackers use scanning tools to choose target computers and access file systems
- Attack usually launched late at night when organization least prepared to deal with it
- Deployment tool released to copy files across network and encrypt as much information as possible before presenting organization with ransom demand
- Ransom payments made in bitcoin, a digital cryptographic currency without a central bank
- Bitcoin market capitalization around $10 billion in Q2 2016
- Approximately 49% of total value of bitcoin transactions associated with illegal activities such as illegal drug trade, pornography, terrorism, money laundering, and capital control avoidance.
- Attackers provide instructions on how and where to buy bitcoin in ransom notes
- Victims can confirm payments and receive decryption instructions via a payment site hosted on the dark web with a timer indicating "time played"
- Three payment options: pay a small fee in bitcoin and receive private key to decrypt one computer; pay full ransom and receive keys to decrypt all affected computers; pay half ransom and receive keys to decrypt half of affected computers (randomly selected by hackers)
- Each option means something different for the victim in terms of remediation
- Little evidence to suggest SamSam attacker ever negotiated on price, and ransom demands have increased over time
- SamSam has brought its hackers over $5.9 million since late 2015, with an average monthly take of around $300,000.

NEXT STEPS

- U of C faced challenges as clock ticked on ransom note: no patient zero found, pressure from board and faculty for open communication and recovery of research, low morale among IT team, sleep deprivation impairing decision-making skills
- Decision to be made on whether to pay ransom; cyber-insurance policy would not cover payment
- Concerns about public reaction if university paid ransom using taxpayer money
- CMT decided to shield SLT and public from fact that situation was a ransom attack
- File recovery excuse involves risk to researchers' privacy and raises questions about how privacy and prioritization should be managed.

********** THE END **********

KLC Samsung-Apple

- Apple and Samsung have been in litigation over intellectual property for almost ten years
- Dispute involves patents protecting components of smartphones, including design patents
- Apple initially sued Samsung in 2011 in the Northern District of California, with Samsung countersuing
- US Patent and Trademark Office tentatively invalidated some of Apple's patents in 2012
- Supreme Court took the case in 2016 and set a standard for defining "article of manufacture"
- In 2014, a jury found in favor of Apple, awarding them almost $120 million for patent violations, but also found that Apple infringed on Samsung's patents, awarding Samsung $158,400
- Samsung appealed to the Federal Circuit, where a panel decided there was no infringement, but this decision was reversed in an en banc hearing
- Overall, Apple has been awarded and settled over $500 million in the litigation with Samsung.

The Technology

- **Apple** has three utility patents related to the design of its iPhone and iPad: '381, '915, and '163
- Utility Patent **'381** covers the spring-back behavior when scrolling a document on an electronic device
- Utility Patent **'915** covers the ability to distinguish between one-finger and two-finger gestures on a touch screen
- Utility Patent **'163** covers the display of electronic documents with multiple boxes of content that can be navigated through touch
- The USPTO has rejected claims of Patent '915 as anticipated by previous patents or unpatentable
- Design patents are less expensive and take less time to file than utility patents, but offer less protection in terms of scope and length of time
- Design patents can be used in actions involving low risk and high reward, depending on balance between limits and advantages
- Design patents do not offer the same level of protection as utility patents in terms of scope or duration
- Design patents are cheaper to file and take less time to be issued compared to utility patents
- **Samsung** has several patents related to communication, music playback, and email transmission technology
- Some of Samsung's patents are standard essential patents, which are required to comply with industry standards
- Samsung's patents cover technology related to MP3 playback, transmitting emails with images, switching between photo and image display modes, and switching between reproduction and photographing modes
- The patents claim specific methods of using the technology, including playing music in standby mode, displaying a single image file after switching between modes, and transmitting messages and images in different email transmission modes

Two Interviews

- Two attorneys were interviewed for their perspectives on a legal battle between two technology companies in the US and Korea

Interview with American attorney

- Apple is known for its focus on design and user interface, while Samsung is known for its manufacturing capabilities
- Apple and Samsung have different business models and approaches to technology development
- Apple is protective of its patents and has in-house patent attorneys
- Samsung formed a patent department in response to infringement lawsuits
- Apple, being based in the US, is familiar with the legal system and has an advantage in filing lawsuits compared to foreign companies like Samsung
- Samsung faced challenges with translation and legal expenses in the US
- The patent infringement case between Apple and Samsung has raised questions about damages calculations and the role of juries in patent cases.
- **The U.S. versus the Korean Legal System**
- American and Korean legal systems differ in terms of process and structure
- Attorneys may have different preferences for jury trials depending on the case
- In patent litigation, it is important to clearly draft claims and specifications
- Apple patents are easier to understand compared to Samsung patents
- Apple was awarded $1.05 billion in damages in a controversial jury decision
- South Korea has a bifurcated litigation system for patent infringement and invalidation cases
- Invalidation cases are heard by the Patent Court, infringement cases by a district court
- **Outcome**
- Samsung gained market recognition and increased brand value as a result of the patent lawsuit
- Samsung gained experience in the US legal system and implemented an in-house intellectual property team to better protect its interests in future cases

Interview with Korean attorney

- Apple is known for its innovative design and GUI for the iPhone, and has a strong focus on software
- Samsung is a manufacturer with a focus on hardware
- Apple has filed lawsuits in the UK and Germany against Samsung products it claims are similar to its own, but these lawsuits have not been successful
- Apple has focused on suing in its home market, the United States, where it is familiar with the legal environment
- Samsung has faced challenges responding to Apple's lawsuits due to language barriers and unfamiliarity with the legal system in the US
- **Damages should be based on the whole product?**
- Damages for patent infringement can be calculated based on the infringer's total profit or a percentage of the infringing portion of the product in the US
- Calculating damages based on total profit may result in overcompensation in cases of design patents in technology-intensive electronic devices like smartphones, which can have over 250,000 patents applied to one product
- This approach to calculating damages may hinder industrial development through innovation

- Alternative method of calculating damages is based on a percentage of the infringing portion of the product
- **Does the scientific knowledge of Jury affect the result of a trial?**
- The jury instruction and verdict form in the Apple vs Samsung case was complex and difficult to understand, even for experts
- The verdict form was 100 pages long and took over 2 hours to read
- The verdict form contained 700 questions
- Juries in the case were composed of laypeople, including electricians, social workers, housewives, and unemployed individuals
- The complexity and difficulty of the jury instructions and verdict form may have been too heavy a burden for the laypeople serving on the jury

Outcome

- Apple and Samsung are two major technology companies
- Apple's strengths are in software, particularly in design and GUI
- Samsung's strengths are in hardware manufacturing
- Apple accused Samsung of copying its products, and filed lawsuits in various countries, including the US and UK
- Samsung was able to increase its brand value and gain the image of a competitor to Apple through the litigation
- Samsung's perspective on patents changed during the litigation, shifting from focusing on the number of patents to improving the quality of patents
- The litigation also led to an improved understanding of patent practices in the US
- Samsung established a patent development group in its telecommunications division after the litigation to handle patent issues related to its products.

********** THE END **********

Building a great place to work

BUILDING A GREAT PLACE TO WORK: INTUIT INDIA

- Intuit India ranked 1st i India among 600 companies
- The business of developing financial software for small businesses, accountants and individuals (intuit india business model)
- Intuit India had ranked number 10 on the list. It had been a steep climb to first place, toppling giants like Google and American Express
- Anand (VP) celebrated the news of topping with all the teams
- Executive Officer of Intuit Inc., often say, “Shareholders are like food — critical to your survival, but you can go three weeks without food. Customers and partners are like water — you can go three days without liquid. However, employees are like air — three minutes and you are done”. These words inspired Anand at every step in his journey to develop a world-class culture to attract, hone and retain top talent.

Company Background

- Intuit was thus built on the idea of listening to customers and delivering products that “wowed” them.
- In 2017, Intuit Inc. had revenues of US$5 billion and around 8,500 employees spread across the world
- 95% of the business came from US rest from other 8 countries
- Its workforce was predominantly made up of top tech talent hired from India’s premier colleges and supported by functional groups in the areas of Human Resources, Finance and Marketing.

Indian IT Industry: Hiring Challenges

- There was a mismatch between the skills required and skills available as their second most critical challenge
- On the one hand, there was an abundance of certain skills, and on the other, there was complete shortage of vital new age skills such as AI ML
- A study found that there was a strong correlation between employee experience and the financial performance of companies.

The GPTW Framework

“In great workplaces, something happens that transcends policies and practices. It isn’t what the companies are doing, it is how their leaders are doing it. And one cannot predict that organizations with the most creative practices, the best bottom line, the least stressful jobs or the most generous compensation packages are the ones that employees will most appreciate.”

Intuit India: The Beginning

- Cook said to anand “we will not tell you what to do you will tell us what is good for intuit we will give you our vision”
- Until 2008 the Great Place to Work GPTW framework was relatively unknown to Intuit India employees.

- The following year, it started to benchmark itself against the industry's best practices and align its own employment practices with them
- The GPTW assessment became a benchmark to demonstrate the progress Intuit India was making in comparison with the best of the best companies in the industry

Culture of listening

Intuit, a company focused on building systems that enable and empower employees to express themselves, implemented an annual employee survey to gather anonymous and candid feedback on the company's diverse themes such as engagement, innovation, leadership, strategy, and career development. However, in 2016, the company increased the frequency of the survey to three times a year and renamed it "Pulse" to gather more timely feedback.

Experienced hires:

Intuit developed the "Assessing for Awesome" framework to efficiently recruit experienced talent. Top employees, called "Awesome Assessors," identified the best candidates for a role based on necessary skills and values

Performance management:

Intuit implemented a "High Performing Organization Review" (HPOR) system for performance management, which included activities such as reviewing and analyzing talent, identifying talent gaps, and preparing talent for promotion. Employees had regular "monthly check-ins" with their managers to review and update goals and discuss progress and performance, using the Situation-Behavior-Impact model to provide feedback.

Recognition and Rewards :

- Paid trips
- Employees who were deemed role models were awarded with gift vouchers

Diversity and Employee Networks:

- Intuit to launch "Intuit Again", an initiative to help female technologists who wished to restart their careers after a break, upskill themselves through a six-month internship and subsequently find meaningful opportunities at Intuit and elsewhere in the industry

- The "Intuit Ability Program" was another attempt to create employment opportunities for persons with disabilities.

Benefits:

- Intuit provides a range of benefits to its employees in India, including free transportation, free food, advanced technology for work-life flexibility, extended maternity leave, special accommodations for expectant mothers, flexible workload policies for new mothers, paid caregiver's leave, financial wellness support, and incentives for high performing employees. The company also offers a contribution to the National Pension Scheme.
- Intuit provided their employees with best working infrastructure gaming zones,cafeteria and etc.

The role of Leadership:

Intuit India's employee engagement scores had been declining prior to 2008, when Anand took over as site head. In an effort to improve the scores and foster a better work culture, Anand embraced vulnerability and asked for help from his team, leading to a more collaborative and open work environment. He also established the India Directors Forum, a group of leaders who could share successes and challenges and support each other's growth. Additionally, he implemented the ILEAD community, which encouraged managers to be vulnerable and transparent about their pain points in order to improve through collective experience sharing and learning. Anand also made an effort to understand the products his company was building by setting up a technology environment for QuickBooks Online and seeking help from a new hire. These efforts helped to improve employee engagement and build a positive work culture at Intuit India.

Intuit Hiring Criteria: What the Company Looks for in a Candidate
Cultural Fitment:

- Values
- Drive for customer success
- Ability to thrive in an environment of fun
- Know their strengths and gaps and are self-aware
- Relationship management skills, given a people-centric organization

Skill Set Fitment:

- Hold of the core skill set
- New technology trends awareness
- Business acumen

Behavioral Fitment:

- Pragmatic thinking
- Self-starter
- Decision-making
- Pragmatic thinking
- Change management
- Ability to think beyond boundaries
- Behavior as a team player
- Self-awareness and openness to feedback

Intuit Values:

- **Integrity without Compromise**
  We speak the truth and assume best intent. We value trust above all else. We hold ourselves and others accountable to the highest standards in all we say and do.
- **We Care and Give Back**
  We are stewards of the future and will do our part to make the world a better place. It is our privilege to help others and we do it wholeheartedly.
- **Be Bold**
  Solve big customer problems. Create a vision that inspires. Think beyond what is accepted as possible.
- **Be Passionate**
  Personally embrace and role model change. Inspire with your insights and initiative. Strive to perfect your craft every day.

- **Be Decisive**
  Choose what we will and will not do. Be transparent with your logic and judgment. Be direct and respectful.

********** THE END **********

Data privacy in India

The Personal Data Protection Bill (DPB) in India aims to regulate the collection, processing, storage, usage, transfer, protection, and disclosure of personal data of Indian residents. The DPB is significant because the digital economy in India is expected to reach a valuation of $1 trillion by 2022 and will attract many global players. While the DPB is similar to the EU's General Data Protection Regulation (GDPR), it also has additional provisions that treat data generated by Indian citizens as a national asset, store and guard it within national boundaries and reserve the right to use it to safeguard defense and strategic interests. The DPB will require companies to change their business models, practices, and principles, and may also add operational costs and complexity. This highlights the increasing importance of data protection regulation around the world.

Privacy as the fundamental right:

- Every citizen provides some of his/her data in order to process in the digital world
- DBP intends to protect and safeguard citizen's privacy rights
- Companies used to exploit and sell user data.
- Companies have to change their business model if they want to keep their place in the market

User consent:

- DPB requires that a digital company must obtain explicit permission from a user before collecting their personal data
- For example Uber ascertains traffic patterns and Amazon analyzes feedbacks from individual transactions using user's data
- Companies should grant the user permission while collecting data and also during the processing of their data

Ownership of personal data:

- DPB proposes that the data provider is the owner of their own personal data.
- This data policy can be a burden for digital companies
- Just like a property owner can ask for his/her property anytime from the person who he/sher has given/rented his property same goes with the data ownership
- Any action the user request to his data is to be performed by the company such as deletion or updation of data

Three classes of data:

- Sensitive data includes information on financials, health, sexual orientation, genetics, transgender status, caste, and religious belief.
- Critical data includes information that the government stipulates from time to time as extraordinarily important, such as military or national security data.
- General data includes the generic information about the user such as name etc
- Sensitive data should be stored in the servers located in India
- Critical data cannot be taken out of the country at all

Data sovereignty:

- DPB will treat citizen data as a national interest
- Currently digital companies own the citizens data and they have to provide any information regarding user data if government demands

National Intrest:

- This DPB doesn't apply to any agency of government in respect of processing of such personal data.
- Government will not seek any permission from user while collecting and processing user data.

Verification Tag:

- Digital companies should verify all the user data they collect from them
- Facebook has millions of fake users and it is not able to verify them

Compliance and enforcement:

- In case of data breach or a minor violation the penalties could reach $700000 or 2% of the company global revenue which ever is higher.
- For major violations, such as data shared without consent, the penalties would double

********** THE END **********

Breach of agreement/ iGate

iGATE Corporation filed a lawsuit against its former CEO, Phaneesh Murthy, in 2014, seeking compensation for damages due to Murthy's behavior. In 2013, Murthy was forced to resign amid allegations of sexual harassment and filed a lawsuit against iGATE, accusing the company of breach of agreement and defamation. Murthy claimed that his contract was unjustifiably terminated "for cause," allowing iGATE to withdraw from its obligations and withhold Murthy's benefits.

iGate Corporation:

- iGate offered IT services globally
- The company provided e-business solutions, application maintenance outsourcing, data warehousing solutions, and enterprise resource planning (ERP) package implementation services, among other services

Murthy's journey with iGate:

Phaneesh Murthy was the CEO of iGATE Corporation, an IT services company. After joining the company, he implemented strategies to position it as a competitive player in the market, including creating a new pricing model based on business outcomes rather than billable hours. Under his leadership, the company's financial metrics improved significantly, with the operating margin growing from -0.2% in 2006 to 18.9% in 2010 and the return on equity rising from 1.5% in 2006 to 23.6% in 2010. Murthy was instrumental in transforming iGATE from a staffing firm to a globally visible software services provider.

ACQUISITION OF PATNI COMPUTER SYSTEMS:

- HIghest achievement of Murthy was the acquisition of Patni
- Merged Patni with Igate and made iGate a billion-dollar entity
- He wants to serve his customers with the best services
- Murthy received bonus and compensation for the achievement

Firing Murthy

- On May 20, 2013, iGATE terminated Murthy’s employment as president and CEO
- He was found in a relationship with a subordinate employee and a claim of sexual harassment
- According to Igate policy if any two employee become involved in romantic or sexual relationship than they must notify this to the higher authority
- The board appreciated Murthy for his contributions to they company but they have to fire him due to violation of policy
- Gerhard Watzinger was appointed as the interim CEO of iGATE with immediate effect
- After the news of Murthy’s firing broke, iGATE was criticized widely and its shares fell

MURTHY’S IMMEDIATE RESPONSE:

Phaneesh Murthy, the former CEO of iGATE Corporation, was terminated from his position amid allegations of sexual harassment. After his termination, Murthy held a teleconference with journalists in India, denying the allegations and calling them "completely false." He claimed that his relationship with his subordinate, Araceli Roiz, was "more than a friendship" but denied that it constituted sexual harassment. Murthy also stated that he had informed the chairman of the company, Ashok Wadhwani, about the relationship after it ended, and maintained that he had not violated company policy. Despite his denial of the allegations, Murthy was later removed from the board of the company with the consent of the majority of shareholders.

MURTHY VS iGate

Seven months after his firing, Murthy filed a lawsuit against the company in a California court, accusing iGATE of breach of agreements, making false promises, withholding wages, and defaming him. Murthy claimed that the company had improperly used its policy on reporting relationships to terminate him, despite knowing about his relationship with a subordinate. He sought compensation for withheld vested stocks valued at $18.3 million, termination benefits of $1.6 million, and monthly medical benefits of $6,000 for 15 years. Murthy also claimed that iGATE had made repeated defamatory statements about him to investors and the public, damaging his reputation.

iGate vs MURTHY:

After Phaneesh Murthy, the former CEO of iGATE Corporation, was terminated in 2013 amid allegations of sexual harassment, the company faced several challenges that inhibited its growth. It also lost a $200 million outsourcing agreement due to management uncertainties and delays in starting the project. In 2014, iGATE filed a countersuit against Murthy, seeking compensation for damages caused by his actions and irresponsible behavior, as well as legal fees and other costs incurred to resolve a claim brought against Murthy and the company by Araceli Roiz. Murthy disputed iGATE's claims and stated that he was entitled to his vested stocks and medical benefits, believing that his termination was "wrongful and unfair." The case received significant media attention and it was uncertain which party would be able to prove their claims in court.

********** THE END **********

Apple Inc. v. Samsung Electronics Co.

- In the spring of 2011, Apple began litigating against Samsung in patent infringement suits, while Apple and Motorola Mobility were already engaged in a patent war on several fronts
- By August 2011, Apple and Samsung were litigating 19 ongoing cases in nine countries; by October, the legal disputes expanded to ten countries
- By July 2012, the two companies were still embroiled in more than 50 lawsuits around the globe, with billions of dollars in damages claimed between them
- While Apple won a ruling in its favor in the U.S., Samsung won rulings in South Korea, Japan, and the UK. On June 4, 2013, Samsung won a limited ban from the U.S. International Trade Commission on sales of certain Apple products after the commission found Apple had violated a Samsung patent,

Origin:

- On January 4, 2007, 4 days before the iPhone was introduced to the world, Apple filed a suite of 4 design patents covering the basic shape of the iPhone. These were followed up in June of that year with massive filing of a color design patent covering 193 screen shots of various iPhone graphical user interfaces
- Apple sued Samsung that it has copied its trademarks, user interface and style.
- Samsung counter-sued Apple in courts in Seoul, Tokyo and Mannheim, Germany, British High Court of Justice, in the United States District Court for the District of Delaware

South Korean courts:

Court issued ruling that Apple had infringed upon two Samsung technology patents, while Samsung violated one of Apple's patents("bounce-back" effect in iOS). The court awarded small damages to both companies and ordered a temporary sales halt of the infringing products in South Korea; however, none of the banned products were the latest models of either Samsung or Apple. Apple's claims that Samsung copied the designs of the iPhone and iPad were
deemed invalid

Japanese courts:

- Court ruled that Samsung's Galaxy smartphones and tablets did not violate an Apple patent on technology that synchronizes music and videos between devices and servers
- Also awarded legal costs to be reimbursed to Samsung.

German courts

- Germany granted Apple's request for an EU-wide preliminary injunction barring Samsung from selling its Galaxy Tab 10.1 device on the grounds that Samsung's product infringed on two of Apple's interface
- After Samsung's allegations of evidence tampering were heard, the court rescinded the EU-wide injunction and granted

- lesser injunction for samsung that only applied to the German market
- Dismissed the ownership of "slide-tounlock"
- Samsung did not violate touch-screen technology patent

French and Italian courts

- After the release of the iPhone 4S, Samsung filed block further Apple iPhone sales in France and Italy, claiming the iPhone infringed on two separate patents of the Wideband Code Division Multiple Access standard.
- No result is written in document

Dutch courts

- Photo gallery app in Android 2.3 was indeed infringing a patent
- Import ban of three Samsung telephones (the Galaxy S, Galaxy S II, and Ace) running the infringing
- software.[3
- Samsung counter-sued and asked the court for an injunction on sale Apple's iPad and iPhones, on the grounds that Apple does not have the licenses to use 3G mobile technology.[
- On October 14, the court ruled, denying the sales ban and stating that because 3G was an industry standard, Samsung's licensing offer had to meet FRAND (fair, reasonable and nondiscriminatory) terms.[40] The court found that Samsung's fee was unreasonable, but noted that, if the companies cannot make a fair and reasonable licensing fee,
- Samsung could open a new case against Apple
- Rejected Apple's claim that Samsung's Galaxy Tab 10.1 infringed its design rights

Australian courts

The injunction Apple sought to block the Tab 10.1 was denied by the
High Court of Australia.

British courts

- British judge ruled Samsung's Galaxy tablets were not similar enough to be confused with Apple's iPad.
- Apple is required to publish a disclaimer on Apple's own website and in the media that Samsung did not copy the iPad

U.S. courts

First U.S. trial

- Apple accused Samsung of infringing on three utility patents and four design patents
- Samsung accused Apple of infringing on United States Patent Nos …

First trial verdict

- verdict largely favorable to Apple. awarded Apple $1.049 billion in damages and Samsung zero damages in its counter suit. Jury found Samsung infringed Apple's patents on iPhone's "Bounce Back Effect", "On-screen Navigation " ,"Tap To Zoom" and design patents that covers iPhone's features such as the "home button, rounded corners and tapered edges
- jury had miscalculated US$400 million in its initial damage assessment and ordered a retrial

Injunction of U.S. sales during first trial

- injunction Apple sought in the U.S. to block Samsung smartphones such as the Infuse 4G and the Droid Charge was denied.
- The preliminary injunction was granted in June 2012, preventing Samsung from making, using, offering to sell, selling, or importing into the U.S. the Galaxy Nexus and any other of its technology making use of the disputed patent.
- On October 11, 2012, court agreed and vacated the injunction.[g into the U.S. the Galaxy Nexus and any other of its technology making use of the disputed patent.

First trial appeal

- On Friday, September 21, 2012, Samsung requested a new trial from the judge in San Jose arguing that the verdict was not supportedby evidence or testimony, that the judge imposed limits on testimony time and the number of witnesses prevented Samsung fromreceiving a fair trial, and that the jury verdict was unreasonable
- Apple filed papers on September 21 and 22, 2012 seeking a further amount of interest and damages totaling $707 million.
- On October 2, 2012, Samsung appealed the decision to the United States Court of Appeals for the Federal Circuit, requesting that Apple's victory be thrown out, claiming that the foreman of the jury had not disclosed that he had been sued by Seagate Technology Inc., his former employer, and which has a strategic relationship with Samsung,

First trial controversy:

- The jury's decision was described as being 'Apple-friendly'
- Questions were raised about validity of US patent system and also the qualification of jury member were deemed in adequate.
- Jury foreman Velvin Hogan was an electrical engineer and a patent holder himself.
- As the jury instructions stated that jurors can make decisions based solely on the law as instructed and "not based on your understanding of the law based on your own cases,"

- the damages award should put the patent holder in approximately the financial position it would have been in had the infringement not occurred"
- The jury was given more than 700 questions, including highly technical
- matters, to reach the verdict and awarded Apple more than US$1 billion in damages after less than three days of deliberations
- Critics claimed that the nine jurors did not have sufficient time to read the jury instructions
- A juror stated in an interview that the jury decided after the first day of deliberations that Samsung was in the wrong

First Retrial of damages amount from first U.S. trial

- US$379.8 million amount that Apple claimed that it is owed in the wake of Samsung's—
- Samsung presented a figure of US$52 million.
- jury awarded a new figure of US$290 million

Supreme Court decision of First Trial

On December 6, 2016, the United States Supreme Court decided 8-0 to reverse the decision from the first trial that awarded nearly $400 million to Apple

Second Retrial of damages amount from first U.S. trial

The parties were ordered to propose a schedule for a new trial by
Wednesday, October 25 ,2017.

Second U.S. trial

- Apple filed a new U.S. lawsuit in February 2012, asserting Samsung's violation of five Apple patents
- Samsung responded with a counterclaim, stating that two patents for nine phones and tablets have been infringed on by Apple
- Samsung stood to gain US$6 million if the jury rules in its favor while Apple was seeking US$2 billion in damages
- The trial began in early April and decision was delivered on May 2, 2014 and Samsung was instructed to pay US$119.6 million to
- Apple for smartphone patent violations
- Samsung appealed the jury verdict to a three-judge panel and won in February 2016, with the panel nullifying the jury verdict
- The panel unanonymously argued that one patent cited by Apple was not infringed by Samsung, while two others, related to autocorrect and "slide to unlock" features, were invalid based onexisting prior art.
- Apple requested an *en banc* hearing from the full District Court panel, which ruled in favor of Apple by an 8-3 decision, restoring the $120 million award, in October 2016

- While the original three judges maintained their opinion from the previous hearing, the remaining judges argued that the three-member panel had dismissed the body of evidence from the jury trial supporting that Apple's patents were valid and Samsung was infringing upon them
- Samsung appealed to the Supreme Court, but the Court announced in November 2017 that it would not hear the appeal, leaving the District Court's ruling in Apple's favor in place[.

********** THE END **********

Deloitte Cyber security roles

Who are Cyber Professionals?

Individuals responsible for protecting an organisation’s network, infrastructure and computer systems.

3 Must Have Skills for Cybersecurity Professionals

1. A strategist to ensure protection of network, infrastructure and computer systems.

2. People management and communication skills to ensure effective coordination with teams and clients. He/she needs to communicate with every professional within an organization about the terms of IT.

3. Technical competency. One should always re-skills with advanced technology skills in order to be capable of grasping

Roles and Responsibilities

- Developing and designing security architecture
- Managing security measures and performance
- Operating regular inspections of system and network processes for security updates and potential breaches.
- Conducting audit process for initiating security and safety measures and strategies.
- Customizing access to information as per identity and necessity.
- Maintaining and improving information security policy, procedure, services and standards.

Why is there a shortage?

There are no signs of the bad guys limiting their talent pools and cybercrime is now a US$445 billion industry with a trajectory of possibly trillions.

To illustrate, toolkits developed by cyber criminals have adapted cloud and managed service business models to propagate and expand cyber criminal activities. These toolkits are easily obtainable with no formal education required to learn how to use them. The revenue from the sales of these toolkits go on to fund more elaborate schemes designed to create chaos and opportunities to rob organisations of their assets.

Cybercriminals are becoming more organised and aggressive while the good guys are struggling to fill their ranks.

In short, the frequency of successfully executed cybercrimes as a result of current day open network society, coupled with the use of cloud services and applications, have created an urgent need in organisations to rapidly advance their cybersecurity countermeasures.

Cybersecurity experts who possess the knowledge, education and most importantly, the thought process necessary to confront the difficulties that accompany the constantly evolving cyber activities are in demand to tackle the challenges posed in the cyber world.

What can you do?

Here are some suggestions on what organisations can do to address the shortage of cyber security professionals

Re-examine your workforce strategy by recognizing the qualities required to run a successful security program and expand hiring efforts beyond career fairs to include polytechnics, local universities and any other avenues.

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. Keeping new hires engaged by giving them the freedom to work on different projects allows them to apprehend new technologies and services.

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

With cybersecurity being a highly dynamic field, continuous learning and upskilling are required to **develop a strong culture of risk awareness**.

Cybersecurity is a complex career field with extraordinarily challenging problems, but with a diverse pool of experiences and ideas, we stand a much better chance of successfully defending our assets.

********** THE END **********

A Comprehensive Approach to Cyber Resilience

- Interviewed 57 tech leaders about cyber threats during 2020
- Cyber resilieince(to handle unexpected disruption) is not restricted to IT team
- Dire need of a plan in how to manage all aspects of data and cross-functional responsibilities to keep data safe

Disruptions Continue to Grow

- Due to work from home in 2020, IT team did not know which device was being used by whom which resulted in weak security arrangements.
- Cyber attacks rose to 400%
- 1000 organizations were interviewed and only 44% had incident response plan of which only 32% said that the plan was actually effective.
- Recent example is solar wind attack on government and fortune 500 companies.

The importance of Data Mangement

- Data Mangement is the process of storing, maintaining, accessing data.
- We should ask following questions while addressing data management issue

- Where does the data come from, and where does the data reside in the organization — for example, in databases, data warehouses, or data lakes?

How frequently does data change, and how does it move throughout the organization over time?

Who (such as IT staff members) or what (internet-of-things devices, or processes from another network) has access to data?

How is data used? For example, is it transformed in some way or fed in raw form to critical systems in the company?

In a crisis such as a natural disaster, how can data be easily accessed or locked down?

If the organization faces a cyberattack, how is the data checked to determine whether it has been compromised? How does the organization trace the flow of contaminated data across the IT architecture?

A cross functional approach to Cyber Resilience

- Matlab ye ke har banda responsible ho data security ke lie not just IT dept
- requires up-front planning to model scenarios that will reveal how data is to be accessed, along with all possible touch points to the organization's network (such as supply chain nodes).
- cross-functional approach across key roles are
  1) Chief data officer: The CDO has overall responsibility of data. Responsible executive-level decisions about data management, both during normal operations and in a possible breach.

  2) Data stewards: has firsthand knowledge of his or her department's data requirements. They know which employees require access to specifc data in order to do their jobs

3) IT team : including cybersecurity engineers and enterprise architects, are the gatekeepers of data. They define the paths by which data comes in or out of corporate systems, along with security protocols

4) HR: The HR function has data about security clearances and work schedules, work-from-home policies, and employee requirements such as virtual private networks.

5) Legal team : The legal function (including staff members working on acquisitions and partnerships) coordinates with the CDO to ensure that vendors have agreements in place stipulating realistic response times in the event of a crisis

6) Other consultants: include people like software engineer to assess vulnerability in software, Enterprise engineers spot redundancy in hardware etc.

7) Machine learning and AI: Last, cyber resilience planning requires not only skilled threat analysts but also advanced algorithms, Machine learning and AI. these solutions can spot irregularities and emerging threats more quickly than human operators, and at lower costs

In the end, whatever steps we take, they should not make people face difficulty doing their work and they at same time maintains the integrity of data