In general, there are three main causes of data breaches: Physical theft, skimming, and cybercrime.

## 1. PHYSICAL THEFT

Physical theft is exactly what it sounds like: A criminal physically steals information. This could mean that a computer, server, or mobile device is taken, or that physical records, such as receipts and customer file, are taken without authorization.

**Summary of the candidate case**:

Employee Stole 'Yandex Search Engine' Source Code, tried to sell it for just $29K.

**Reason for choosing this story:**

The reason for me to select and study about this security breach is my previous company and its work culture. Employees are scanned thoroughly every day when they enter and leave the office. I did think it was not good way of approach to not believe the employees and doing this all day made me to have a very bad impression on my company policies. But when I came to know about this, I was totally shocked and thus realized that there are also people who do sell the company's software for money making a huge loss to the company and that also impacts all the employees in that company.

**Story:**

Yandex is the most popular search engine in Russia and is a big rival of Google. Its market share in November 2015 reached around 57 percent of all search queries within Russia, compared to Google's 35.2 percent. A former employee of Yandex allegedly stole the source code and key algorithms for its search engine site and then attempted to sell them on the black market to fund his own startup.

Russian publication Kommersant reports that a former employee of Yandex Dmitry Korobov downloaded a type of software nicknamed "Arcadia" from Yandex's servers, which contained highly critical information, including the source code and some of the "key algorithms," of its search engine and then attempted to sell the stolen codes for $25,000(which actually cost around $15 Million USD) to an electronics retailer called NIX, where a friend of his allegedly worked, and on the dark underground market in search of potential buyers.

However, Korobov was arrested by Russia's Federal Security Service (FSB) before any transaction could take place. If he had been succeeded, the code of Yandex's core service was floating freely over the Internet, resulting in serious consequences for the company. The report noted that Korobov's court hearing took place earlier in earlier December 2015, and he received a suspended sentence of 2 years in jail after being accused of illegal possession as well as the distribution of commercial secrets.

**How it is related to network security:**

Physical theft presents a real risk to data, it's important to treat physical security with the same level of attention as cybersecurity.

**Steps to impose Security:**

The security can be achieved by monitoring and restricting access to data storage and processing areas, enforcing strict policies regarding BYOD and remote access, developing policies regarding the locking and protecting of computers and mobile devices, and training employees to be aware of suspicious activity. Strict policies that govern the disposal of old data are also important; thieves are not above searching through the garbage to find useful information.

**URL:**

http://thehackernews.com/2015/12/search-engine-source-code.html

## 2. SKIMMING

Skimming is the theft of data contained in the magnetic strip on the back of a credit or debit card.

**Summary of the candidate case:**

Malicious software infected point-of-sale systems at Target checkout counters.

**Reason for choosing this story:**

This is one of the breach that is closely related to my family. We did shop in Target about 20 days before this breach happened. After coming to know about this we immediately cancelled the Credit card and also checked the activities on the credit card. But unfortunately, we had a suspicious activity of $250, which was then refunded from the bank. This is an unforgettable one as this was the first time it happened and we didn't exactly know what to do until we contacted our bank.

**Story:**

In an interview with CNBC on Jan. 12, Target CEO Gregg Steinhafel confirmed that the attackers stole card data by installing malicious software on point-of-sale (POS) devices in the checkout lines at Target stores. A report published by Reuters that same day stated that the Target breach involved memory-scraping malware.

This type of malicious software uses a technique that parses data stored briefly in the memory banks of specific POS devices; in doing so, the malware captures the data stored on the card's magnetic stripe in the instant after it has been swiped at the terminal and is still in the system's memory. Armed with this information, thieves can create cloned copies of the cards and use them to shop in stores for high-priced merchandise.

**Steps to impose Security:**

Protecting POS terminals against skimmers relies on vigilance, and close monitoring to prevent tampering. Experts recommend regularly opening or disassembling the terminal to ensure that it has not been compromised; if evidence of tampering is found, there is a chance of data breach and need to respond accordingly.

**URL:**

http://www.securityweek.com/target-confirms-point-sale-malware-was-used-attack
http://krebsonsecurity.com/2014/01/a-first-look-at-the-target-intrusion-malware/

## 3. CYBERCRIME

Cybercrime is, overall, the most common source of data breaches. This includes cyberespionage, Web application attacks, denial-of-service attacks, malware, and viruses.

**Summary of the candidate case:**

Ukrainian Power Grid: Hacked

**Reason for choosing this story:**

This is the first time I'm coming to know about a hack on a power grid. When I heard about this news, I was thinking for couple of minutes that even power grids are being hacked and what benefit does the hacker get in hacking a power grid and shutting down the power supply of a whole country. Later when I started to study on this I came to know there are people who do hacking just for publicity, hobby and passion as well. People doing this may sometime end up in prison wasting their rest of life. Later, I realized that a lot a talents are being wasted this way and took my attention on this story.

**Story:**

Ukrainian news outlet TSN first reported on the Dec. 23, 2015, power outage, which it said left about half of all homes in the country's western Ivano-Frankivsk region without power for a few hours. It said that government investigators believed that the outage was tied to a "virus" that had been employed as part of a "hacker attack" that involved remote access to industrial control systems at a local energy supplier called Prykarpattyaoblenergo.

Slovakian information security firm ESET says the malware used in the attacks was the BlackEnergy Trojan, which has previously been tied to Russian attackers, and which is often used to install additional attack modules on victims' systems. After infecting these ICS systems, for example, this particular BlackEnergy variant was then designed to install wiper malware called KillDisk, which overwrites or deletes data on hard drives and can also render them unbootable.

Researchers said hackers had used backdoors to spread the KillDisk wiper module through booby-trapped macro functions embedded in Microsoft Office documents across the Ukrainian power authorities.

Therefore, it is believed that the initial point of infection with BlackEnergy caused after employees opened Microsoft Office files containing malicious macros.

**Steps to impose Security:**

Protecting against cybercrime is a major priority for any company that collects customer information, and usually involves ensuring that virus protection is kept up to date, installing intrusion detection and prevention software, maintaining firewalls, keeping logs of activity on sensitive networks, and following industry standards for data protection.

**URL:**

http://www.databreachtoday.com/ukrainian-power-grid-hacked-a-8779
http://thehackernews.com/2016/01/Ukraine-power-system-hacked.html