Case Studies:

The True Cost of Cyberattacks

The average data breach cost companies **$3.8 million** in **2019**. There are four major areas of cost when your organization is the victim of a data breach or other cyberattack:

1. **Loss of trust:**
   Customers no longer feel their data is safe in your hands.

2. **Removal and cleansing of systems:**
   This is the actual cost to remove the malware, pay a ransomware demand or restore damaged data.

3. **Value:**
   Bad public relations is always a bad thing for the stock value of a publicly traded company. In addition, a long downtime and loss of service to customers can affect short-term profits and long-term customer retention.

4. **Penalties and fines:**
   In the European Union, companies can be fined €10 million, or up to two percent of global revenue per incident, whichever is higher. California recently passed similar regulations.

Here's a look at the impact of some larger cybersecurity incidents in recent years.

Atlanta City Government Ransomware Attack

In March 2018, the IT systems of the Atlanta city government came under attack. Earlier in the year, a report had noted more than **1,500 vulnerabilities** in the city's systems. The attack, from a group of Iranians known as SamSam, used a brute-force attack to transmit simple passwords in the hope of finding an account with an easily guessed password. It succeeded and managed to encrypt the data systems for the city, including the personal information of six million residents.

The group asked for a **ransom of $52,000 in Bitcoins**. The city did not say if it had paid the ransom, but it appeared to have never received the decryption key.

Many city services across five separate departments, including public WiFi at the airport, bill payment and other functions were offline for five days while the systems were cleansed and restored. Eventually – in some cases months later -- much of the lost data and systems were restored from backups, but at great cost. **The initial contract to do this work and further secure the systems was for $2.3 million, but eventually the total cost was closer to $9 million.**

FACC Whaling Attack

FACC, an Austrian aircraft parts manufacturer, was tricked into sending $56 million to a criminal's account. The spear phishing of a high-level executive – known as **"whaling"** – used a fake email to impersonate a high-level executive and request the transfer.

This type of attack is known as a "business email compromise" or "fake president scam." The employee who fell for the trick, the head of finance and the CEO **were all fired**. The company's **stock took a 17% dive** on the news.

The key fact here is that the cybersecurity technology was not compromised. The email looked legitimate, but the attackers did not appear to have actually accessed the internal email system at the company. The individual responsible for the transfer simply didn't notice that the message wasn't real.

The FBI notes that these types of incidents cost companies more than **a billion per year**.

The Mirai Botnet Attack

In October 2016, major websites such as PayPal, Twitter, Netflix and Spotify suddenly weren't available. A company called Dyn, which supported the Domain Name Servers (DNSs) for these providers (essentially an Internet address book that allows you to access web services) was receiving 1.2 terabits of requests each second from **millions of devices**.

These devices were all "smart" devices, or part of the Internet of Things (IoT). This includes printers, digital video recorders, smart TVs, baby monitors and dozens of other similar devices.

IoT devices include simple computers that usually run a Linux operating system. A piece of Malware known as Mirai had spread itself all over the world and **infected millions of devices**. It was programmed to automatically check default passwords and if one worked it would load itself into memory and wait for a command. The devices still worked properly, but the malware was running alongside the normal functions.

Then, one day the creators of Mirai turned all the devices on at the same time and formed a "botnet" or network of controlled devices. These devices started issuing DNS requests to Dyn and the sheer volume of them brought down several major services.

This type of attack is called a Distributed Denial of Service attack. Recovering from the loss of business while your system is inaccessible can **cost up to $2.3 million** for certain types of businesses.

Equifax Data Breach

In 2017, hackers exploited an unpatched security flaw in the credit dispute website run by Equifax.

From there, they accessed usernames and passwords of internal employees and for the next 76 days they accessed the names, social security numbers, birthdates, addresses and more **from 143 million Americans**.

Equifax eventually closed the security flaw after detecting the intrusion, but not before its data (which included 200,000 credit card numbers) was stolen.

In total, the breach **cost Equifax $1.4 billion** plus legal fees.