Ethics and Security

Assignment 2

Submitted by

Basavraj Jaliminche

Student Id-8800149

Date-2022-07-25

Q.1 Find an example of a security breach from a news report from the past three months. Please do not use any examples that have been given in class.

Describe the breach in your own words and identify the elements and categories of the breach as discussed in class. Additionally, identify the attack vectors used. Recall the differences between elements, categories and vectors all discussed in class.

Answer:

# Data breach at Toronto health network possibly exposed patient information, OHIP numbers

## Leak affects patients at Scarborough Health Network hospitals prior to Feb. 1

A Toronto health network says some of its servers containing a variety of personal patient details were recently breached.

The Scarborough Health Network (SHN), which includes three hospitals and eight satellite sites, said in a statement Wednesday their IT department first noticed "unusual activity" on its servers Jan. 25. Its investigation with cybersecurity experts found past and present patient data may have been accessed.

"We take the privacy and security of business contact and personal information very seriously, and sincerely regret that this Incident occurred," the network said in its statement.

"We can confirm that the unauthorized actor was shut out of the system by February 1, 2022. Patient data from February 1, 2022 and onward is not at risk."

The leak may have impacted anyone who received in-patient care at an SHN hospital prior to Feb. 1, whose data would have been collected for their chart.

The hospital network said it couldn't determine which patients were specifically affected but that it included patients who received care prior to the amalgamation of SHN Centenary Hospital (also known as Scarborough Centenary Hospital), SHN General (also known as Scarborough General), and Birchmount Hospital (also known as Scarborough Grace) under one network in 2016. It also affects patients who received care at hospitals that were part of the former Rouge Valley Hospital Network, including RVHS Ajax and Pickering Campus or Ajax-Pickering Hospital.

Those who only visited a COVID-19 clinic affiliated with SHN were not affected, as their data was uploaded to provincial ministry servers.

## 'No indication' data has been misused: SHN

The health network says large swath of information may have been accessed, including their patients' names, dates of birth, marital statuses, home addresses, phone numbers, email addresses, OHIP numbers, insurance policy numbers, lab results, diagnosis information, COVID-19 immunization records. Staff names and numbers may have also been accessed.

There is "no indication that any personal information potentially accessed in connection with the incident has been misused in any way" to date, the hospital network said in the release.

But due to the nature of the information, SHN is warning of potential identity theft and phishing attempts and says it will not contact anyone by email requesting payment or other sensitive information. They've also notified Ontario's information and privacy commissioner about the incident.

SHN is also offering a two-year subscription to an online fraud monitoring service through TransUnion to all current and former patients, which can be activated anytime before Sept. 30 by calling the SHN call centre.

This data breach is possibly due to

### 1. Compromised Credentials

**‍**Usernames and passwords are still the most common type of access credential and continue to be exposed in [data leaks](https://www.upguard.com/blog/data-leak), [phishing scams](https://www.upguard.com/blog/phishing) and by [malware](https://www.upguard.com/blog/malware). When lost, stolen or exposed, credentials give attackers unfettered access. This is why organizations are now investing in tools to continuously monitor for [data exposures and leaked credentials](https://www.upguard.com/product/breachsight). Password managers, [two-factor authentication](https://www.upguard.com/blog/two-factor-authentication) and [biometrics](https://www.upguard.com/blog/biometrics) can reduce the risk of leak credentials resulting in a security incident too.

### 6. Ransomware

**‍**[Ransomware](https://www.upguard.com/blog/ransomware) is a form of extortion where data is deleted or encrypted unless a ransom is paid, such as [WannaCry](https://www.upguard.com/blog/wannacry). Minimize the impact of [ransomware attacks](https://www.upguard.com/blog/what-is-ransomware-as-a-service) by maintaining a [defense plan](https://www.upguard.com/blog/best-practices-to-prevent-ransomware-attacks), including keeping your systems patched and backing up important data.

### 7. Phishing

**‍**[Phishing](https://www.upguard.com/blog/phishing) is a [social engineering](https://www.upguard.com/blog/social-engineering) technique where the target is contacted by email, telephone or text message by someone who is posing to be a legitimate colleague or institution to trick them into providing [sensitive data](https://www.upguard.com/blog/sensitive-data), credentials or [personally identifiable information (PII)](https://www.upguard.com/blog/personally-identifiable-information-pii). To minimize phishing, educate your staff on [the importance of cybersecurity](https://www.upguard.com/blog/cybersecurity-important) and prevent [email spoofing](https://www.upguard.com/blog/email-spoofing) and typo squatting.

Q.2 Choose a tech related company and research their impact (positive, negative, or both) on the environment. Include at least two suggestions of ways they could sustainably improve their environmental impact. Remember to provide full and proper citations.

Answer:

Tandem :

As software engineers and product designers creating custom digital projects, it’s easy to forget about all of the resources that go into making your job possible. Think of the “Cloud” — out of sight, out of mind. But the resources and energy used to build your computer, power it, and power the data center holding your information in the Cloud all contribute to carbon emissions.

Because software is intangible, it can be difficult to grasp how it affects the environment. The [Information and Communications Technology (ICT)](https://www.tutor2u.net/business/reference/what-is-ict) sector is rapidly growing, accounting for [more than 2% of global emissions](https://www.nature.com/articles/d41586-018-06610-y) — roughly the same as the aviation industry’s carbon footprint from fuel emissions. The environmental impact has become too big to ignore, and the increasing number of devices, expansion of data centers, and ambiguity of carbon offsets all contribute to the problem. It’s not all bad news, though with thoughtful research and planning, there are solutions company can work toward to initiate change.

### An Increasing Number of Devices Means An Increased Need for Energy :

Right now, the ICT sector makes up over 2% of global emissions, but if trends continue, by 2040 it will constitute 15% of global emissions: equivalent to [half of the entire world’s transportation sector](https://www.eng.mcmaster.ca/news/study-shows-smartphones-harm-environment) emissions. One reason for that is the rapid growth of the Internet of Things (IoT) — or the system of internet-connected, “smart” physical objects collecting and exchanging data via a wireless network. Juniper Research reported that the number of IoT connections will rise from 35 billion in 2020 to [83 billion in 2024](https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024), which is 130% growth in just four years. And by 2023, [66% of the global population](https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.pdf) will have internet access (compared to 51% in 2018).

As more and more people get connected, the question is whether or not there will be enough electricity to power all these devices. Fossil fuels and nuclear power are the main sources of electricity in the US, both of which are finite resources. Moreover, the data centers that house these vast amounts of information require lots of electricity, and with more devices in the world, there will have to be more data centers.

### The Expansion of Data Centers

The rise in the number of devices and cloud-based services has led to an expansion of data centers, which consume [2% of the world’s electricity](https://hbr.org/2020/09/how-green-is-your-software). By 2030, that number could be 8%.

“Data Center Alley” is a little-known tech hub that processes [70% of global internet traffic](https://www.washingtonian.com/2016/09/14/70-percent-worlds-web-traffic-flows-loudoun-county/). Companies like Amazon, Google, Apple, and Microsoft own or rent data centers in Data Center Alley. Amazon dominates the world of cloud-computing real estate, owning enough data centers in the area that [nearly a third of the internet runs on Amazon Web Services](https://www.forbes.com/sites/danrunkevicius/2020/09/03/how-amazon-quietly-powers-the-internet/?sh=3de7a8653092) (AWS). Because of this, many tech companies and their stakeholders want their cloud-computing services to be hosted close by for the quickest service and updates.

However, what tech companies don’t realize is that while AWS may try to dedicate resources to powering their operations with renewable energy, the source of electricity for data centers [is completely dependent on the local region](https://datacenterfrontier.com/data-centers-becoming-larger-players-in-power-markets/). In this case, Data Center Alley is reliant on Loudoun County, Virginia’s resources: a utility provider called Dominion Energy that happens to run on [mostly fossil fuels](https://www.wired.com/story/amazon-google-microsoft-green-clouds-and-hyperscale-data-centers/). This leads to the conundrum that faces many tech companies, who are put in a position of having to choose between being on the bleeding edge and being sustainable.

As of 2020, AWS has established [5 carbon-neutral zones](https://youtu.be/iEUPwHyIOBQ?t=945) where they purchase carbon offsets to balance the emissions coming from those zones. However, this solution is more complex than meets the eye.

### The Ambiguity of Carbon Offsets

To combat the negative effects of their carbon emissions — and, perhaps, the negative public perception of those emissions — it has become increasingly popular for companies like Amazon to purchase carbon offsets. A carbon offset is a reduction in greenhouse gas emissions (like carbon dioxide) used to compensate for emissions made somewhere else. When someone buys a carbon offset, the money goes toward a project that removes greenhouse gases from the atmosphere or prevents new emissions. The most common carbon offset projects are forest management or renewable electricity generation initiatives. Individuals and organizations can buy carbon offsets to balance the scale for emissions they can’t reduce themselves.

There are two offset categories: mandatory and voluntary. Mandatory offsets, also known as compliance offsets, are purchased because of a legally binding limit to the amount of greenhouse gases that an organization can release. On the other hand, individuals and organizations purchase voluntary offsets at their discretion. As of 2019, the mandatory offset market was [$44 billion](https://www.washingtonpost.com/business/energy/why-carbon-offsets-dont-do-all-that-they-promise/2020/08/15/4480f11a-deb4-11ea-b4f1-25b762cdbbf4_story.html), while the voluntary offset market was around $300 million.

When it comes to purchasing carbon offsets, there are many concerns. First, [there is no globally recognized price](https://www.washingtonpost.com/climate-solutions/2020/09/23/climate-curious-advice/) for carbon offsets, so the price of buying a carbon offset is often much lower than the actual cost of climate damage caused by emissions. Furthermore, there is no federal regulation of voluntary offsets, so individuals must do their own research to ensure the offset company delivers what they promise. For instance, the Vatican was once presented with offset certificates to make their governing body carbon-neutral — but the millions of trees promised [were never actually planted](https://yaleclimateconnections.org/2019/05/are-carbon-offsets-a-scam/).

# What Can We Do About It?

### Responsibly Purchase Carbon Offsets

Purchasing carbon offsets is better than not doing anything at all — however, it’s important to do your research. When seeking a company to buy offsets from, look for a portfolio of permanent and enforceable projects and certifications, and it’s even better if a third party has accredited the projects. Ensuring the projects benefit the communities where they are located, rather than placing additional stress on them, is imperative. Above all, transparency is key.

When purchasing carbon offsets, purchase more than necessary, if possible. For example, if your team has to fly to another city for a conference, buying two or three carbon offsets for each person (rather than just one) will make your carbon footprint fall rather than only stop it from going up. With some initial groundwork, you can find a carbon offset company and project that aligns with your business values.

### Start a Conversation

A great way to start a conversation about the environmental impact of your work is to make thoughtful decisions about where your company’s data is stored. The first step to creating change is learning whether company data is stored in a carbon-neutral zone or a zone contributing to greenhouse gas emissions. [The Green Web Foundation](https://www.thegreenwebfoundation.org/) is a resource that shows what websites (including your own) are hosted by a certified green company. Migrating your company’s data to a carbon-neutral region is a big lift, but it doesn’t take too much effort to start a conversation about it and explore what a migration would require.

If you work for a larger company with an enterprise account linked to a data center running on fossil fuels, ask the data center’s account manager for more renewable options. Another excellent way to take action is by signing petitions (and creating them!). Ultimately, educating yourself and getting the conversation started will help shed light on the environmental impact of the tech industry.

Q.3 You are consulting for a financial institution that wants you to put together a training session for their employees on security. Research three instances (these should not be ones shared in class or used elsewhere in this assignment) in which attackers used social engineering to attempt to gain access to a system. Describe the approach they used.

Answer:

The term "social engineering" is used to describe a wide range of malevolent behaviours carried out through interactions with other people. Users are duped into divulging critical information or committing security blunders via psychological manipulation.

Attacks by social engineers may involve one or more steps. To prepare for an assault, a perpetrator first looks into the target in order to learn background details like probable points of entry and lax security measures. The attacker next makes an effort to win over the victim's trust and offer incentives for later security-breaking activities, such disclosing confidential information or allowing access to vital resources.

Social engineering tactics for attack

Attacks using social engineering can be carried out anywhere there is a chance of human interaction. The five most typical types of digital social engineering attacks are listed below.

Baiting

As the term suggests, baiting attacks use a fictitious promise to spark a victim's curiosity or sense of avarice. In order to steal their personal information or infect their systems with malware, they trick users into falling for a trap. encouraging the installation of malicious software or software that doesn't do anything but enrich the criminal. Scareware is also known as fraudware, deception software, and rogue scanner software.

A typical scareware example is the legitimate-appearing popup advertisements that show up in your browser while you're browsing the internet and say things like, "Your computer may be infected with nasty spyware applications." Either it offers to install the programme for you (which is frequently malware-infested), or it directs you to a dangerous website where your PC is infected.

Spam emails that give customers offers to purchase useless or dangerous services or that issue fictitious warnings are another way that scareware is disseminated.

Pretexting

Here, an attacker gains knowledge by telling a string of cleverly constructed lies. The con is frequently started by a perpetrator who poses as someone who needs the victim's private information to complete a crucial task.

The assailant typically begins by gaining the victim's trust by posing as a coworker, police officer, bank or tax official, or any person with the authority to know something. Through queries that are allegedly necessary to verify the victim's identification, the pretexter collects crucial personal information.

This fraud is used to obtain all kinds of important data and records, including social security numbers, individual addresses and phone numbers, phone records, dates of staff vacation, bank records, and even security data pertaining to a physical plant.

Phishing

Phishing scams, one of the most common forms of social engineering attack, are email and text message campaigns designed to make victims feel rushed, curious, or afraid. Then it prompts people to divulge private information, click on links to nefarious websites, or open attachments that are infected with malware.

An illustration would be an email sent to subscribers of an online service informing them of a policy violation that necessitates quick action, like a necessary password change. It contains a link to a malicious website that looks almost exactly like its legitimate counterpart and asks the unwary user to enter their current login information and a new password. The information is delivered to the attacker upon form submission.