Cybersecurity Presentation 2
Casey Adams

Charleston Southern University

CSCI.405

T-Mobile Data Breaches

- T-Mobile experienced at least two data breaches in the year 2023. According to Labus from helpnetsecurity.com, the company first reported the data breach on January 19.
- (Labus) "The breach exposed the personal information of approximately 37 million customers. According to T-Mobile, the hackers were able to access the data by exploiting a single Application Programming Interface".
- APIs enable two software components to communicate and some APIs can have vulnerabilities that attackers might exploit to gain unauthorized access, execute commands, or steal data.
- T-Mobile said in this breach that, "No credit card information, passwords, Social Security numbers, government ID numbers or other financial account information was exposed in the breach".

Another Data Breach

- T- Mobile experienced the another data breach in the year 2023. (Labus) "The attack started on February 24 and lasted until March 30, and affected 836 customers".
- T-Mobile revealed that, “In March 2023, the measures we have in place to alert us to unauthorized activity worked as designed and we were able to determine that a bad actor gained access to limited information from a small number of T-Mobile accounts between late February and March 2023”.
- The company said that no personal financial account information or call records were compromised. This again was caused by exploiting a single Application Programming Interface at a different chain of T-Mobile stores which seems there is a lack of security protocol in different chains of T-mobile.
- This is why they are continuing to use an outside 3rd party IT company to secure their data.

And Even More Data Breaches

- Unfortunately, T-Mobile has had several breaches over the recent years, A November data breach in 2022 exposed 37 million customers data.
- This included names, billing addresses, emails, phone numbers, dates of birth, T-Mobile account numbers and information describing the kind of service they have with the wireless carrier.
- Another notable T-Mobile breach happened in August 2021 affecting 49 million customers.
- Although when initial reports first come out explaining what type of data was breached, sometimes later they find out that more data was exposed then first stated. This is why there is a need to keep up-to-date on the breach to see if anything has changed in the reporting and the effects of the attack.

Some Outcomes of Breaches

- Because most breaches can go unnoticed for days, weeks, or even months, customers are not aware they need to be on guard for possible phishing scams or monitor their accounts for fraudulent activity.
- Because of that reason the attackers most likely were getting away with many smaller to mid size fraudulent transactions for months.
- This is all the more reason to always be on guard for phishing scams and always monitor all accounts regardless if your company that you use has reported a data breach.

How Users Can Protect Themselves

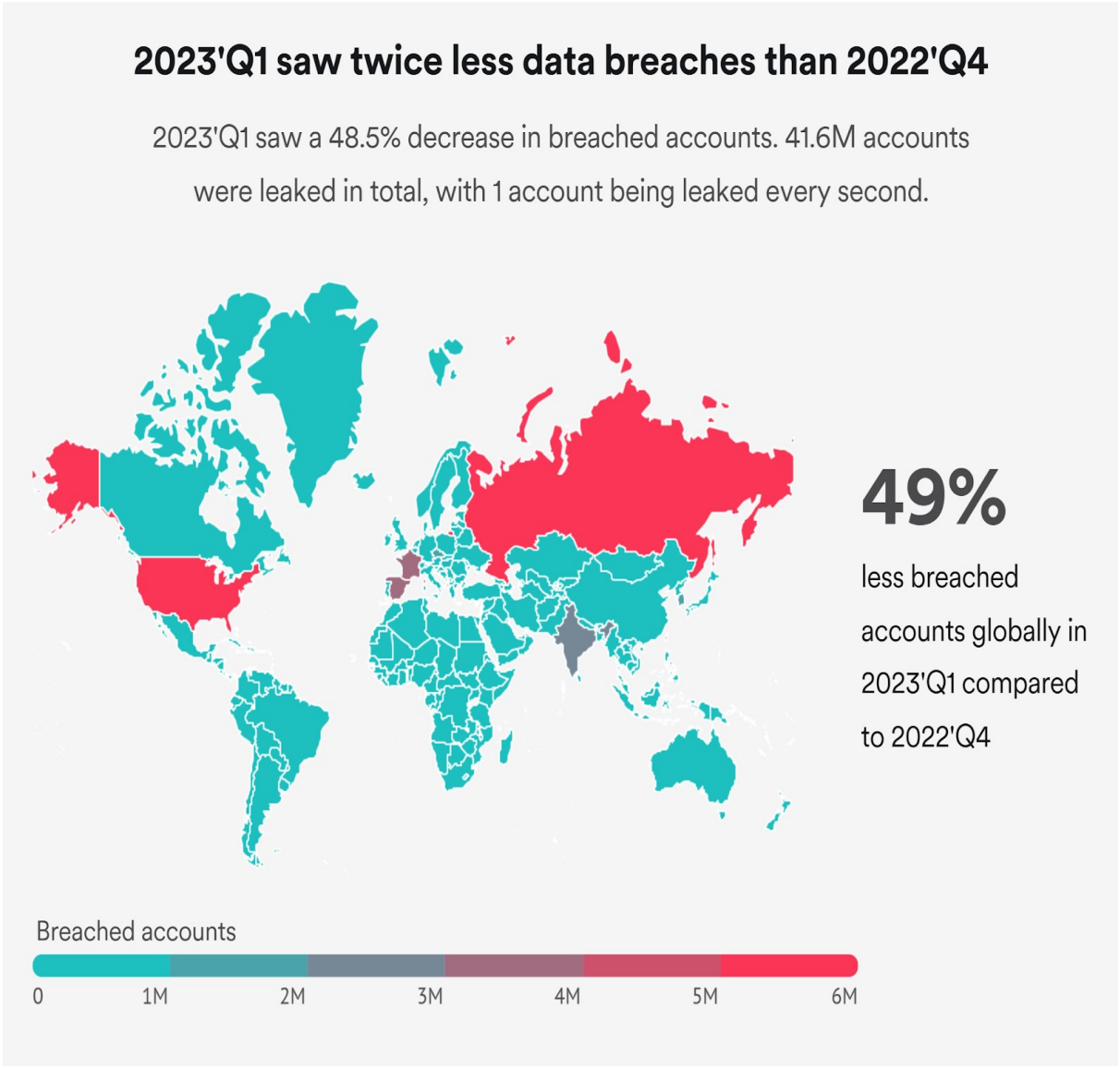
- The average user can avoid becoming a victim to an attack by always be on guard for phishing scams, not clicking on unknown links, keep personal devices and work devices separate, and never give information over the phone or via email to someone that reaches out to you asking for personal information such as passwords, email, PINs, social security numbers, etc.
- If you reach out to someone always be sure to verify you are speaking with the correct person before giving out any personal information. Be sure to only give out the information that is needed, you do not want a business to have more of your personal information than they need to have.
- proactively change your PINs, passwords, monitor all accounts on a regular basis.
- Make sure all devices are being updated regularly including anti virus, firewalls, web browsers, OS updates, and any other updates that your computer reminds you of.

How Businesses Can Protect Themselves

- Larger businesses should always have an up to date IT department. Outside 3rd party IT companies are also a good option so there is more accountability with the company.
- Keep the network and any software such as firewalls, antivirus, and individual devices up-to-date.
- Businesses should limit peoples permissions on what they can do on a work device such as not being able remove important software on the device because they did not understand its importance and ensuring employees cannot download anything they want.
- There should also be different subnets in larger businesses that way if there were to be an attack it can help to contain it.

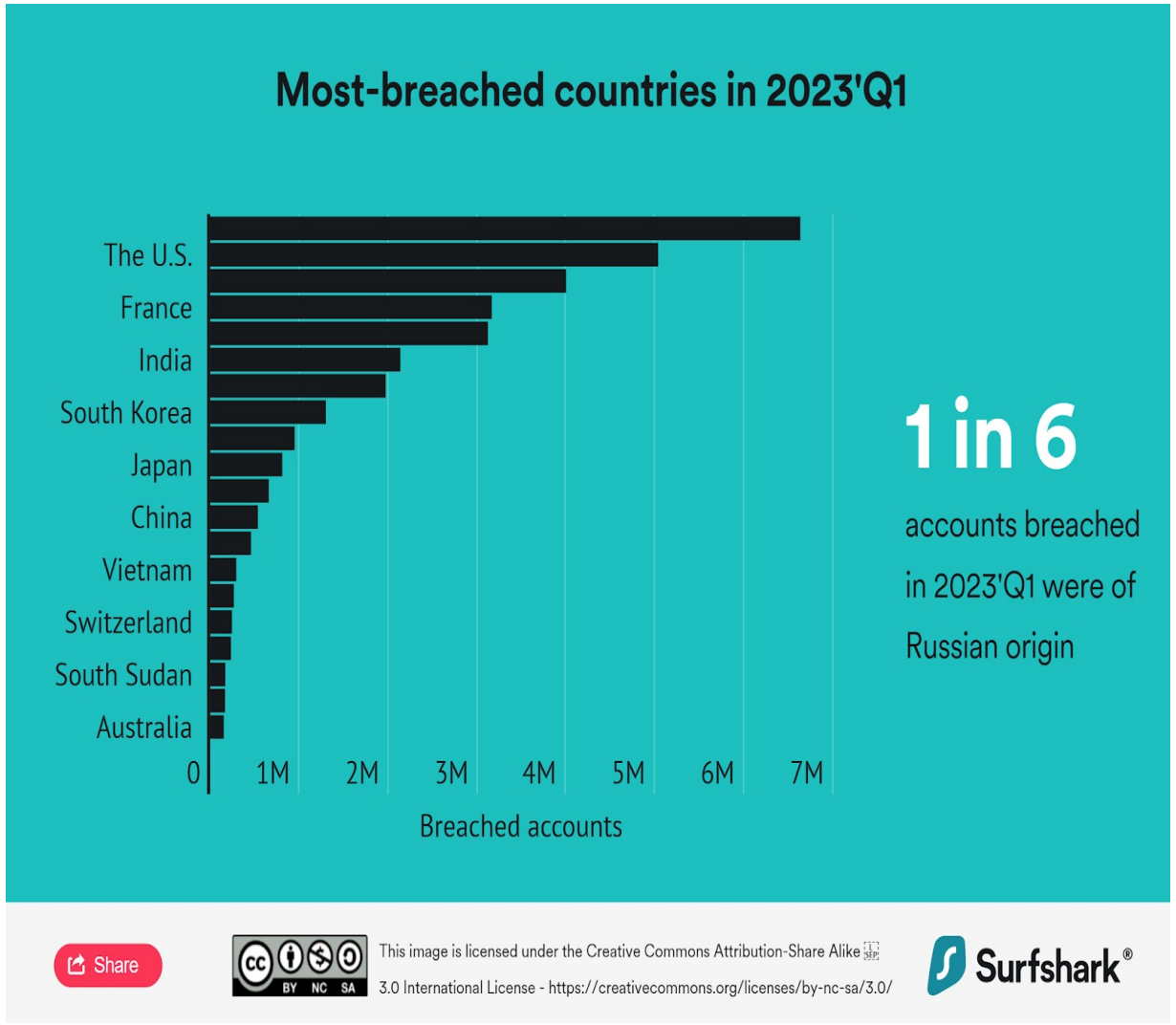
Data Breach Chart

This Chart was provided by Dr. Hura Anwar on Digitalinformationworld.com. It shows us that there is a downward trend in breaches from 2022Q4 to 2023Q1. As we can see in the chart Russia and the United States are being hacked the most.



Second Chart

This Chart was also provided by Dr. Anwar. This chart lets us see closer to the exact number of breaches and also informs us that 1 and 6 breaches are coming from Russia.



Regions and Sectors Affected by Breaches

- Dr. Hura Anwar also broke down the number of breaches by region. Dr. Hura says the most vulnerable region is Europe with 17.5 million leaked accounts in the past quarter, larger than all other regions.
- (Anwar)” Europe happened to be the sole region that showed a quarter-over-quarter rise in data breach statistics. It nearly doubled from Q4 of 2022 to Q1 of 2023.”
- Some of the biggest data breaches happened in sectors like banking, groceries, insurance, payments, and computer technology education.

Conclusion

- The T-Mobile attacks show just how relentless hackers are. T-Mobile shows us just how many times any company can be attacked, even a large company like them. One of the larger breaches of T-Mobile was caused by an exploiting an application program interface, as we discussed on earlier slides.
- Hackers can send out phishing emails hoping people will click on a link or social engineering and trick someone to get them information by lying about who they are or what their purpose is. With the amount of times T-Mobile has been hacked it seems like they have a break down in communication, standards, and protocol. The same attack has been used just at different T-Mobile locations. It sounds like they need to retrain everyone about best practices and continue getting help from their 3rd party IT company to fix any and all APIs they currently use.
- We can learn from T-Mobiles mistakes but T-Mobile is not the only large company attacked multiple times. As we saw earlier there are many large countries being attacked or attacking networks every second of everyday.
- Learning about all this information is very important so people are educated which will mean less breaches are happening just as we discussed in slide 8.

References

- Electric.ai. (July, 2023) "High Profile Company Data Breaches 2023". https://www.electric.ai/blog/recent-big-company-data-breaches

- Labus, Helga. (May, 2023) "T-Mobile suffers second data breach this year". https://www.helpnetsecurity.com/2023/05/03/t-mobile-breach-2023/

- Zorz, Zelijka. (August, 2021) "T-Mobile data breach: New information uncovered by the investigation". https://www.helpnetsecurity.com/2021/08/18/t-mobile-data- breach-information/

- Anwar, Hura. (May, 2023) "Global Data Breach Statistics In Focus: Where Do The Trends Stand In 2023?". https://www.digitalinformationworld.com/2023/05/global-data- breach-statistics-in-focus.html