The case that I chose is the famous hack on Sony that started in late 2014, which can be found here: https://www.riskbasedsecurity.com/2014/12/05/a-breakdown-and-analysis-of-the-december-2014-sony-hack/. This case made the news due to the drastic scale that it took place on. In addition, this breach isn't something that just happened over a weekend and then was over. Instead, this breach still had lasting ramifications in 2018 that affected countries on a global scale, at least in some way.

This breach was a data breach that leaked personal information of all the employees of Sony, all of Sony's purchases and expenditures (some which were odd in nature, like purchasing movie tickets to Sony movies just to give them to all their employees), and much more. The hack was done by a group that goes by the name of GOP, or The Guardians of Peace. It hit the news and suspicion for the hack lay on North Korea's shoulders, since a recent Sony movie called "The Interview" was inflammatory toward North Korea, enough so that North Korea said they would consider the movie "an act of war" if it were released. If it were North Korea's doings, this movie would be evidence as to why they were a target for the hackers.

Naturally, there are many threats to this breach, and even more so depending on how you view the potential threats. One threat that is obvious is the safety of Sony's employees, since in this breach, many thousands of Sony's employees' social security numbers were released to the public and GOP sent threatening remarks to employees of Sony saying they and their families would be in danger if this didn't completely disassociate from Sony altogether. As time went on with this hack, more and more data kept being released. If the vulnerability in the code allows the hacking to go unresolved, this would continue to place all of Sony's assets and all its employees in danger. If North Korea really was behind it or continued to act like they were, then

this ongoing hack could also put pressure on global relations, which could be potentially catastrophic in its reach.

The hack originated from infected files on employees' computers. From there, the hackers were able to access a backdoor to Sony's servers. After that, they were home free. To stop this sort of attack in the future, developers could enact a policy where they scan files that enter employee computers to ensure that each file is what it says it is. Additionally, developers could close the backdoors in the system and only allow access to certain files only when it is necessary, i.e. zero trust. A zero trust policy will certainly help prevent this type of attack in the future.

The best practices for this Sony breach would be to enact tighter security on the files that are allowed within employee computers, since files had to become infected in the first place in order to spread this virus around. Authentication of employees only to the degree they need authentication would help prevent this sort of attack in the future, since the hackers would have to have access to an employee that has the required authentication instead of just anyone if they were to hack again in the future. The same thing applies for authorization, since all those in high-ranking roles would certainly be authorized to access data that must remain secure. Therefore, they should be wary and ensure that they only access websites and emails that are not infected and are not phishing. Accounting should allot more funds to their cyber security department to give Sony employees better training in how to stay away from phishing links or other vulnerabilities. Additionally, they would need a stronger cybersecurity team to strengthen their defenses against potential hackers in the future. Lastly, they should enact the defense in depth technique of cybersecurity. Every layer of their access to the internet and to important files/file networks (such as their servers) should be properly encrypted, scanned for phishing

links, and secured in more than one way. If one trap doesn't stop potential hacker's attempts to phish or otherwise compromise files or data of an employee's, another trap should, which is the glory of the defense in depth technique of cybersecurity.