# Cybersecurity: Are We Really Safe? The SolarWinds Hack

Of the world's biggest problems, cybersecurity is a big one. However, due to its widespread repercussions should it be neglected, it is largely paid attention to. But in March 2020, a large hack - Russian in origin - destroyed that barrier of false security built up by a decade of trust in cybersecurity. Three companies - SolarWinds, an information technology (IT) company, Malwarebytes, a cybersecurity and antivirus company, and FireEye, a hub of cybersecurity for some of the world's most important companies and information - were broken into. On the matter of these break-ins, first we'll cover what cybersecurity is, then go in-depth about the break-ins, and finally discuss the potential long-term consequences of theses break-ins.

Cybersecurity is the ever-present and overshadowing function of the keeping safe of our data on various technologies. Initially, it sufficed to encrypt data by encoding it - scrambling the data and using a password to unscramble it, sort of like a key for a lock. Encoding is still used today, but has been updated to meet current standards. As it is hard to crack most encryption, provided it follows current guidelines, password cracking bots try billions of different combinations on sites that could contain important data - banks, payment services, and sometimes even password managers - giving them access to a user's credentials for other, sometimes more important sites. However, cybersecurity software is available - although mostly coming with a monetary fee. You may have heard of McAffee or Malwarebytes, antivirus companies that - as indicated by their names - mainly block computer viruses and malware on your computer. But they also can help remind you to strengthen your passwords or to uninstall potentially harmful programs. All in all, cybersecurity is important and yet somehow forgotten about.

SolarWinds, an Information Technology (IT) company, suffered a Russian-originated hack as early as March 2020. This was not an isolated event - the hack actually broke into FireEye, a cybersecurity company, exposing information from the United States Departments of Homeland Security, State, Treasury, and Commerce, as well as the National Institutes of Health. In addition, the antivirus company Malwarebytes reported that it too was a victim of the Russian hack. So this was more than an isolated attack against SolarWinds. However, SolarWinds seemed to be the most unprepared: "It's [SolarWinds'] security practices appear to be lacking on a few fronts, including the use of the password 'SolarWinds123' for its update server," says WIRED's Brian Barrett in an article on the SolarWinds attack (I don't know if the password has been changed since that publication but if not it just adds to the pile). The breach exposed millions of personal health records as well as classified Homeland Security data, and officials are still not sure who has been affected or which information was compromised. In addition, a class-action lawsuit was filed against SolarWinds by a shareholder, alleging that SolarWinds administration "misrepresented and failed to disclose" vital information after the hack. Dissenters argue that dissemination of information - truthful information - could have helped investors and shareholders get out before they suffered excessive stock loss. This was just another addition to the pile - the SolarWinds hackers also viewed Microsoft source code. This means that the hackers could find security vulnerabilities in Windows, Microsoft Office, and potentially even MS-DOS (though that last one is pretty unlikely; MS-DOS has been around for decades and is unlikely to have viable security vulnerabilities) as well as many other Microsoft programs, websites, and more. But this is the tip of the iceberg - uncountable other security vulnerabilities and exposed corporations exist, and are likely suffering the consequences of the hack.

Finally, the long-term consequences of what has been dubbed the "SolarWinds hack" are likely to be devastating. As mentioned earlier, private and important data has been viewed and therefore can give the hackers a lot of potential power over individuals and corporations as well as the United States government, or at least parts of it. Your data specifically could have been compromised or found since the hack. What will be done with the data, or with the vulnerabilities? Even as teams of experienced professionals attempt to clean up whatever breaches can be found, the stolen data could be being put to use to stop them. So this incident, though you might not have heard of it or seen it in the news, is much bigger than many things seen before.

All in all, cybersecurity is a large problem, though not viewed as such in most cases. In addition to the civil unrest and slight instability brought about by the latest transition of power in the government, the SolarWinds hack has created a potential vulnerability; not one of cybersecurity, but one in our nation. I ask you once again, are we really safe?

Sources:
WIRED, "Russia's SolarWinds Hack is a Historic Mess," wired.com/story/russia-solarwinds-hack-roundup/
FOX News, "SolarWinds shareholder files class-action lawsuit," https://www.foxbusiness.com/markets/solarwinds-shareholder-files-class-action-lawsuit
ZDNet, "Malwarebytes said it was hacked by the same group who breached SolarWinds," zdnet.com/article/malwarebytes-said-it-was-hacked-by-the-same-group-who-breached-solarwinds/
TechTarget, "What is the Future of Cybersecurity?"searchsecurity.techtarget.com/feature/What-is-the-future-of-cybersecurity