Rise of Cyber Attacks

Kevin Durand, kdura002

Introduction

With the current state of the world, from climate change ravaging the planet, to the cost-of-living spiraling out of control, there is a lot of dissent I the world that could put cybercrimes on the rise. For most people torrenting videos and games and other media are commonplace, with the lack of general free time and disposable income people are pushed to find what they want in various means. The chance of cyber attacks is more prevalent than ever, just look at the rise of workplace deviance, the increase in cyber-attacks from workers against their company. In some cases, the increasing likelihood of attacks is more worrisome in conjunction with new technology, Crispr technology take information on genes and how to alter them and is a far more dangerous set of information for hackers to gain access to. Using the NIST handbook though, the threat of cyberattacks can be used to the advantage of cyber security professionals, using methodical methods to protect against all cyber-attacks. With the increase in cyber attacks there is more than ever a need for cybersecurity professionals to defend our information from those who wish to steal it.

Workplace Deviance

Workplace deviance is when people at a job use cyber based tactics to steal information from the company or use secured data for their own benefit. With the rise of inflation rising prices while barely moving wages there is a bigger chance than ever that there will be unmotivated workers looking to make ends meet, considering a lot of people are unable to purchase healthy food and homes. When you have unmotivated workers with access to sensitive data you have a higher chance of those works doing cyber-attacks, and the easiest place to do those attacks at is a place you are familiar with. This idea is already cemented into cybersecurity considerations, there is even a term “man in the middle attacks” for that sort of attack, this idea of getting something more from the place you work is nothing new. The topic of man in the middle attacks is also prevalent in modern media; in the movie “Office Space” the watcher finds themselves seeing the life of an individual unhappy with their job with friends unhappy with their jobs, the premise of the movie is that they steal a tiny bit of money from every transaction using a computer bug. If something is such a strong idea that it can show up inside the media of a people, it is clearly something that is prevalent within that society of people. Another way in which office deviance can occur is with the rise of software like chat GPT, while the use of GPT is not really questioned here, the potential things that could happen are. With GPT someone could take sensitive information from their job, put it into Chat GPT to make a better report or write up for them, maybe even process the data; if Chat GPT were to be compromised, it can even be something outside of the software itself, that means that anyone putting company information into that program makes that information viable for theft. With the rising of financial inequities, where workers are treated less and paid less while prices around them soar, you are bound to have more workplace deviance, from stealing company time to stealing company secrets, making workplace deviance a large issue.

Crispr Gene-Editing

Crispr is a gene editing software, it takes genetic information from a donor and can make changes to that DNA using that information. Workplace deviance is not the only place where cyber attacks are on the rise, there are cyber security threats being thwarted all over the place; with the introduction of the very genes of people being information stored on IoT devices, the threat of devastating attacks are only on the rise. The idea behind Crispr is something that is questionable on its own but consider that someone could possibly forge someone's DNA from information they steal; with the right set of information any person could be accused of crimes that they did not commit, have "proof" that someone was somewhere they were not. While there are certainly issues between people, imagine how violated someone would feel if someone could steal their genetic information to use to alter themselves. The other idea is that genetic information can be stolen by other governments, that these cyber threat nations could just simply take whatever information they wanted from an international citizen to cause all sorts of trouble. One good example is imagine if China were able to genetically alter someone to look like another world leader, with genetic information free to be taken that genetically altered person could cause all sorts of havoc acting as that foreign leader. With access to the very genetic building blocks of individuals, the threat to privacy that Crispr offers is potentially infinite; it is the job of cyber security individuals and the companies that use Crispr to make sure that information is completely secured.

NIST Framework

Even with the rise of cyber attacks on businesses and the fact that the most private of information is now possible available to the world with Crispr, following the guidelines of the NIST framework provides an excellent defense. Workplace deviance serves to threaten the security of companies and their information, while Crispr software takes the most private of data to use in its operation; it is more important than ever for companies to have an ablative defense against all sorts of cyber threats, with NIST framework anyone can make a strong cyber security program. In the first section of the NIST framework, there is a great deal of dissemination of information, becoming familiar with the first section provides a good structure understanding of concepts that will be applied in a cybersecurity set up. In the next section the framework goes through the anatomy of an attack, giving a cyber professional access to that information makes it even easier to defend against everything that is out there. In the middle of this section, it gives very plain steps that cyber attacks have to take, almost as if it was an almanac to cyberattacks, this goes over much more in depth the different specific parts of an attack. Lastly the second section gives access to the tiers of cybersecurity and how each tier of that security plays a role in the anatomy of a cyber-attack. Using this information professionals are already informed enough to recognize attacks, especially those on secure information and from inside a business itself. Following the section on the anatomy of an attack, the framework goes into how to form a gameplan in the face of a cyber attack. The professional reading the NIST documentation will have a good guide on how to prepare an ablative defense, by using the information on how an attack is formed, there can be a number of different level of defenses based purely on the levels of attacks.

Conclusion

Cyber attacks are on the rise, from the workplace to overseas state enemies, it is important to recognize the factors that could cause cyber attacks and how to defend against them, and with the very genetic make up of people being using in technology the need to defend private information is larger than ever. Workplace deviance is a specific form of attack that can occur from within a company, people with access to secure bits of information on a system can attack a vulnerable system, cyber security professionals would be good to pay attention to trends like that to stop those kinds of attacks. Crispr gene-editing takes genetic information from donors and allows them to be edited, while editing others with that genetic information potentially, represents information that needs to be protected like no other. With the NIST Framework as a guide a cyber security professional would be able to account for the rise in workplace deviance with a surety that genetic information in Crispr systems is safe and secure.