**How Security Awareness Can Protect the Tech Industry**

The technology industry has often fallen victim to the ever-evolving cyber threats. However, it doesn’t really come as a surprise considering the valuable data these companies hold. Since employees working in tech industry are likely to be early adapters of latest technology, they are also more vulnerable to these attacks until the technology matures. For instance, tech-savvy employees tend to install new apps and use latest smart devices while they are still not secured completely. Because tech products are a part of almost every business, the technology sector sometimes indirectly plays a role in making other businesses vulnerable. Hence, it would not be wrong to say that though technology has made our lives much easier, it has also made us susceptible to security threats. Consider point-of-sale systems where even a small vulnerability can cause data breaches for retailers, or a backdoor in a communication hardware which can result in a number of cyber-attacks.

**Threats faced by Tech Industry**

So, what are the threats that the tech industry faces? Because software companies hold valuable commodities, they can be a big source of business for cyber criminals who sell and exchange stolen intellectual property to public markets. Let us briefly look at some of the threats faced by the tech industry and how security awareness can help protect it.

**Identity Theft**

Many tech companies that provide online services or use Ecommerce platforms for [online transactions](http://www.cardzgroup.com/ScratchCard.html) need customer’s Personally Identifiable Information by country laws. Cybercriminals steal this information and use customer identities for carrying out illegal activities or for their personal monetary gain.

**Loss of Intellectual Property**

If an organization loses intellectual property, it can severely damage its reputation. Sometimes, your competitors are also involved in intellectual property thefts against you as their competition. A much bigger threat can be a malicious insider with the required level of access to valuable information that can be retrieved in a much lesser time.

**Hacktivism**

This threat is particularly related to the tech industry. Hacktivism works when a high-tech organization sues cyber criminals who hack their product and the hackers in return target them in the form of “hacktivist” groups, thus leading to financial losses or reputational damage for the company. For instance, in 2015, Hacking Team, an Italian technology organization that sells spying and hacking software was hacked by Phineas Fisher, who upon being sued, explained that he did so in a goodwill to protect human rights.

**How can a Security Awareness Program Help?**

According to a [survey](https://purplesec.us/resources/cyber-security-statistics/#:~:text=Nearly%2060%20million%20Americans%20have,United%20States%3A%2038%25.), in the year 2019 alone, the global average cost of a data breach was 3.92 million dollars; and an increase of 22.7% in cyber security costs from 2016 to 2017. In the past few years, big companies like Facebook, Quora and Uber have been victim to cyber-attacks resulting in leakage of their valuable customer information. These increasing stats demonstrate the need to create effective security awareness programs which develop methods, techniques and employee competencies necessary to deal proactively with potential security threats. Moreover, security awareness trainings should not be a one-time thing, and conducted periodically for regular improvement in the employees. It holds even greater importance for the tech sector as it is important to keep all the employees on the same page and equally educate technical and non-technical staff. It is pertinent to keep in mind that ensuring security cannot be a one man show and everyone needs to be equally involved to make it successful. Hence, in addition to technical tools used for implementing cybersecurity in a technology company, individual training is as important.

Since technology sector faces greater threats from cyber-attacks, their workforce needs to be more equipped to respond to such threats and stay vigilant at all times.

**Planning an Effective Security Awareness Program**

For any [business](https://www.dailyhostnews.com/things-startups-need-to-know-about-cybersecurity) planning to implement a security program, the first line of defense is how an attack can be prevented with the help of controls. This demands that security best practices including security tools and techniques are completely enforced. Then comes breach detection, which means that once you are under attack, you should have to capacity of timely detection. Lastly, but most importantly, is your employees. You may have all controls of detection and prevention in place, but you still may not be able to successfully face a cyber attack unless your employees are well trained to do so. This is where a security awareness program helps you by working on your third line of defense. It educates your employees about the first and second lines of defense, and how you can mitigate risk during vulnerable times using the right knowledge and tools.

Let’s have a brief look at how a technology company can implement an effective security awareness program.

**Educate Your Employees**

According to Kroll, approximately [90 percent](https://www.venafi.com/blog/7-data-breaches-caused-human-error-did-encryption-play-role) of data breaches were caused by human negligence between 2017 to 2018. The higher management of IT security like governance, risk and compliance managers and other security personnel have to devise information security policies, an essential part of which is employee trainings and awareness sessions. This will ensure that all employees have the right amount of education to avoid potential future threats.

**Develop Security Skillset**

With increasing demand to fill in security positions, the tech sector especially needs to hire and upskill security analysts, penetration testers and security consultants. These job roles can be created out of existing ones such as web developers, network and system administrators, or from entry-level security jobs. To start an information security role, it is essential to learn security frameworks and standards like CISSP, PCI DSS, and ISO 27001.

**Avoid being a Victim of Hactivism**

So how exactly can you do that? You can keep a low profile and use best practices such as deploying a Virtual Private Network, multifactor authentication, firewalls and tools to protect against DDoS attacks. You can also conduct threat simulations to check how employees respond to an actual attack.

**Protect Your Intellectual Property**

Access control is the key if you want your intellectual property to be safe. Limit access to your critical files and only allow authorized individuals after getting them to sign confidentiality statement. Now that your staff is trained and you have hired professionals, deploy the best security technology such as Security Information and Event Management (SIEM) and Data Loss Prevention tools to quickly recognize any outliers. Be proactive and act fast in case of any potential attempt to access your intellectual property.

**In a nutshell,** organizations in the tech industry should protect and safeguard their private infrastructure and deploy productive threat intelligence. It’s not about damage control anymore, rather it’s about how strong your preventive measures are. This is why, developing a culture of security awareness to mitigate threats and creating a preventive strategy is crucial to ensure the success of a technology organization.