Cybersecurity: What to Watch in 2018

It seems that every year brings a new onslaught of data breaches, and 2017 has been no exception, topped by the Equifax breach that involved more than 143 million records.

The frequency of data breaches is not likely to slow down as we enter the New Year. The 2017 Annual Cybercrime Report calls cybercrime "the greatest threat to every company in the world" and predicts that cybercrime will cost $6 trillion annually by 2021. It is essential that companies be up to speed on the major trends and issues shaping cybersecurity in 2018.

Lack of Cybersecurity Talent

One trend from 2017 that will continue into 2018 is the lack of available cybersecurity talent on a global scale. There are thousands of job openings in the United States alone that are sitting unfilled due to a skills gap. The lack of qualified employees is leaving companies short-handed when it comes to security, which is leading many companies to consider outsourcing instead of building an in-house cybersecurity team.

Artificial Intelligence

The lack of skilled workers in cybersecurity has also led to the rise of Artificial Intelligence (AI) playing a larger role in cybersecurity. AI utilizes a combination of machine learning and data and behavioral analytics in order to detect threats much quicker and more efficiently than humans can. Incorporating AI into cybersecurity efforts can also allow companies to bring on a smaller number of staff to manage security issues, which can lead to cost savings as well. However, companies should ideally have both AI protections as well as the human component in order to increase their level of protection.

Employee Training

While the human component is necessary, it can frequently be the cause of many cyber breaches. Unfortunately, employees are often at the root of the problem when a company faces a cyber incident, with many breaches resulting from a phishing email. Companies are implementing BYOD policies to stem the tide of employee-caused breaches, as well as putting restrictions in place to prevent employees from using personal email accounts to transmit proprietary company data. This is why it is becoming even more important for companies to implement cybersecurity training for employees. Cybersecurity training is gaining steam, with many companies choosing to invest in these kinds of programs in the hope of reducing their risk of a breach.

Cloud Security

Companies are also housing more information in the cloud – making cloud security more important. Research conducted by security vendor Ixia indicates that 90% of respondents expressed concern

about security in public clouds. One aspect of cloud storage that companies need to understand is who is responsible for security. That burden typically falls on the customer as opposed to the provider. Companies that use cloud storage for their data need to carefully examine those agreements to ensure that data is adequately protected.

These are just a few of the cybersecurity issues that companies will face next year. Cybersecurity will continue to be a concern for companies as the workplace becomes increasingly digital and the amount of data that companies process continues to grow.