BROOKS PIERCE

Sure, Hindsight is 20/20 But These 2020 Cybersecurity New Year's Resolutions Will Aid in Securing Your Business

12.20.2019

In this day, data is often one of the most valuable assets companies have and it needs to be protected as such. Guarding data has become crucial for every business, no matter the size and industry. In the first half of 2019, there were 3,800 publicly disclosed breaches and 4.1 billion records exposed according to NortonLifeLock Inc, a global leader in consumer cyber safety. To protect your customers and business, here are five tasks we recommend implementing in 2020:

1. Simple Steps

Companies of all sizes are expected to implement "reasonable security measures" and should expect to be held accountable for their data privacy practices. Failure to do so can result in substantial costs in the event of a data breach. While what constitutes reasonable security measures can vary based on industry, the type of data a company maintains, and other basic security measures like strong password requirements, use of firewalls, professional security audits and regular computer software updates can make a significant difference in protecting data. All companies, regardless of size, will also benefit from periodic assessments by legal and technical professionals to make sure appropriate data security measures are in place and the protocols are being followed.

2. Have an Information Security Policy

It is nearly inevitable that your company will suffer some sort of data breach. An information security policy can provide companies with important benefits when responding to a data security incident and be used as a benchmark for training employees on data security and data breach response. A strong policy will include information about how personally identifiable information such as names, birthdates and social security numbers will be collected, stored and shared, how to report a possible data security incident, how customers will be notified of an incident and the appropriate people to spearhead the company's response.

3. Assess Current Methods of Collecting, Retaining and Storing Information

Every business needs to examine the information it collects and saves. From there, determine how long data is being stored, its purpose and if practices are reflective of industry standards. If you learn that your company is keeping data that is not critical to running your business, consider

changing practices to stop collecting and storing it. When discarding or deleting data, be sure to dispose of it safely, securely and in alignment with legal requirements.

4. Prevention Tools

To aid in preventing a breach consider purchasing an intrusion detection system that monitors for malicious activity. If a breach does occur, it could be helpful to have cybersecurity insurance, which can help cover the legal and regulatory costs associated with a breach. When purchasing these products, be sure to determine the best fit for your company based on current data collection, retention and storing methods.

5. Be Prepared for a Breach

Data breaches happen due to hackers and everyday human error, so the amount of time and money you invest preparing for a breach can save you time and money later. Forming a response plan will give your company the tools to react appropriately, minimizing company disruption and a diminished reputation with your customers. If a breach does occur, a speedy approach to securing a team of experts to facilitate the response and notifying regulators and impacted individuals is essential.

PEOPLE

Will Quick

SERVICES

Privacy