Cyber Threats – What Will 2020 Bring?

As 2019 comes to a close, we contemplate what the new year may bring. There are a number of positive thoughts, like financial growth and enhanced customer relationships, but unfortunately there are the negatives as well – one being cyber threats. Threats are increasing and evolving as each year passes, which is why security planning and reviewing plans is a must for any business operation.

Some predictions for 2020 include the following:

1. *Expansion of Ransomware* – Ransomware is a type of malicious software, or malware, designed in part to deny access to a computer system or data until a ransom is paid. As the U.S. Homeland Security Division has reported, ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Recovery can be a difficult process, and there is no guarantee that individuals will recover their files if they pay the ransom.

   In 2019, ransomware increased. Also, criminals are not focusing on the size of the business they want to attack, but more on how adverse an impact would be on a business, in order to get the business to pay the ransom. And, unfortunately, there is no indication that this will let up in 2020, with new versions and types of ransomware attacks being most likely. This means that we will need to be sure to re-evaluate and tighten security because what we do today may not prevent an attack down the road. For example, focus will need to be not only on security of data and proper backup of data measures, but also on protection of applications, as attacks turn to business applications and not just the compromising of data.[1]

   Some precautions to consider with your experts and for your operations, include, but are not limited to:

   - Proper firewalls, anti-virus, and anti-malware programs;
   - Regularly updating and patching software and systems – close your vulnerabilities;
   - Verifying and confirming with a known independent reputable source before clicking on links or opening attachments;
   - Properly back up on a regular basis, and be sure to test backup and determine if it is functioning properly – make sure it is not adversely impacted;
   - Restrict user permissions and access on business systems;
   - Consider intrusion prevention, intrusion detection, and monitoring programs for systems;
   - Scan all incoming and outgoing emails to detect threats and to filter what reaches end users;
   - Identify security practices to secure data and systems, and to handle transfer of funds; and
   - Regularly train and educate all of the individuals in your organization on issues of concern and precautions that they can take.

[1] What cybercrime will look like in 2020, by Marcus Fowler, www.techradar.com, 12/03/2019

2. *Deepfakes and Phishing* – Technology has become more sophisticated, allowing criminals to "deep fake" audio, video, … you name it – where they pretend to be a reputable person, yet it is the criminal. There was a recent report of a criminal using a "deepfake" voice to get money from a company. We need to be concerned, because it is anticipated that this will become more prevalent, with voices getting cloned and tricking staff into thinking that they are being told by their supervisors, for example, to do something like send money or send sensitive information, etc. Also, phishing attempts (email scams) to dupe people will continue as well as the increased use of text messages to accomplish the same.[2]

   So, it is not just email that we need to question; all forms of communication received need to be verified and confirmed when dealing with money and sensitive information, or when asked to click on a link or attachment, for example. Again, training and awareness is key here. Personnel is on the frontline and unfortunately, because they are only human, they are the weakest link. Regularly remind personnel of what is transpiring and identify guidelines to protect your operations. Also, discuss testing options with your experts, in order to determine the level of awareness of personnel.

3. *Other Commercial Targets That May Affect You* – Think about what services you rely on to run your business. Ask if something happened to them how will that impact you? Take cloud providers for example; a lot of businesses rely on them, but they are not infallible. It is anticipated that there will be an increased number of data breaches on cloud providers. As a result, your business needs to focus on security in this relationship. What is the shared responsibility (and realize that responsibilities can change based on whose services and what services you use)?[3] Also, do not forget about your other third-party providers that could have an impact on your operations if their security is not up to the level that it should be – the impact may be devastating to you. Address security with those that touch your business.

For the coming year, again plan accordingly, review plans, educate, and focus on these and other security initiatives. Industry experts are forecasting again that there will be smarter hackers and more breaches. Forecasts are for increased risks, requiring all of us to continually stay on top of our security initiatives from both a technological as well as an administrative level. Because it is an area that is always changing, it requires our constant evaluation and assessment in structuring a successful risk management plan.

If you have any questions on this article, please contact Colleen M. Capossela, President of CATICPro, Inc., 860-513-3131.

---

[2] Legal Departments Should Expect 'Deepfakes,' Phishing Scams to Increase in 2020, by Dan Clark, www.law.com, 12/02/2019

[3] Own Your Cloud Security, by Gary Marsden, https://securityboulevard.com, 10/10/19