Protect your **company** from a **cyberattack**
Have a **respond** & **recovery plan** and **don't forget** to **keep mitigation** a **top priority** for **your employees**

25th anniversary 1997-2022

AMERICA'S SBDC
TECHNOLOGY ACCREDITED
PUERTO RICO
INTER AMERICAN UNIVERSITY

All businesses have confidential information. From personal information of each employee, as well as customers and partners. This information is provided with the assumption of confidentiality and security, so each business must be prepared and have the tools to protect it.

In the age of technology, it is important to know what information must be protected and how, to identify vulnerabilities in the systems, to respond quickly to an attack, and if necessary, to recover the information as soon as possible.

There are different threats that businesses must be alert to. From viruses that damage the confidential information; spyware that gathers users information; and/or malware made to gain access to a company's protected systems. In addition to compromising the confidentiality of a company's information, all of the above examples have the disastrous consequence of damaging the image and reputation of a company.

How to protect your company from these attacks? The National Cybersecurity Alliance recommends the following steps:

Identify what data you actually need to collect and what is the critical confidential information of your business. Ensure that the data is encrypted, know who has access to the data and that it is being tracked by your business.

Protect your network using complex passwords changing them periodically. Avoid using the same passwords on multiple accounts.

Disaster Recovery

Add **Multi Factor Authentication** with administrator logins to delay or stop attacker's efforts to gain administrative access to your systems. Place **firewalls** around critical data to protect your network from unwanted visitors. Always Update your software to reduce the chances of your system being compromised.

To detect possible problems, maintain a continuous monitoring for unusual activity, malware, and/or active attacks. Remove data abnormalities and respond in an appropriate and timely manner. Use **antiviruses** and encryption software on all your devices. Do not open any attachments or click links from unknown sources.

Have a **respond & recovery plan** prepared, making your own encrypted **backups** and consider how to isolate them to prevent deletion or destruction.

Don't forget to keep mitigation a top priority for your employees. Create a culture of security by implementing a regular schedule of employee training. Cybersecurity in the Workplace is Everyone's Business. Bring up to date employees about new risks and vulnerabilities. Consider blocking employees access to the network if they don't attend.

If your company does not have the capacity or personnel with the necessary knowledge to keep your information secure, **hire professionals** with those skills. Consider hiring independent **forensic investigators** to help you determine the source and scope of any breach. Consider hiring **outside legal counsel** with privacy and data security expertise.

RESOURCES

AmericasSBDC.org/Cybersecurity StopRansomware.gov FTC.gov

https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity/basics
https://staysafeonline.org/wp-content/uploads/2018/10/NCSA_2018_Week3.pdf

PUSHING BIG ON THE LITTLE ONE
Knowing the seminars offered in 2022 or request business assistance you can access **negociospr.org**

Business Plans • Federal Contracting
Marketing • Access to Capital
International Trade • Innovation and Technology

Arecibo 787.878.5269
Barranquitas 787.857.3600 ext. 2101
Caguas 787.744.8833 ext. 2909

Fajardo 787.863.2390 ext. 2360
Ponce 787.284.1912 ext. 2023
San Germán 787.892.6760

San Juan 787.763.5108
Executive Office 787.763.6811
International Trade 787.763.2665
Innovation and Technology 787.763.6922

CAGUAS

DEPARTAMENTO DE DESARROLLO ECONÓMICO Y COMERCIO
DDEC

POWERED BY SBA
U.S. Small Business Administration

Funded in part through a Cooperative Agreement with the U.S. Small Business Administration.

INTER