The Official Publication of the MIDJersey Chamber of Commerce

midJersey BUSINESS

midjerseybusiness.com

2015 MIDJERSEY REAL ESTATE REPORT

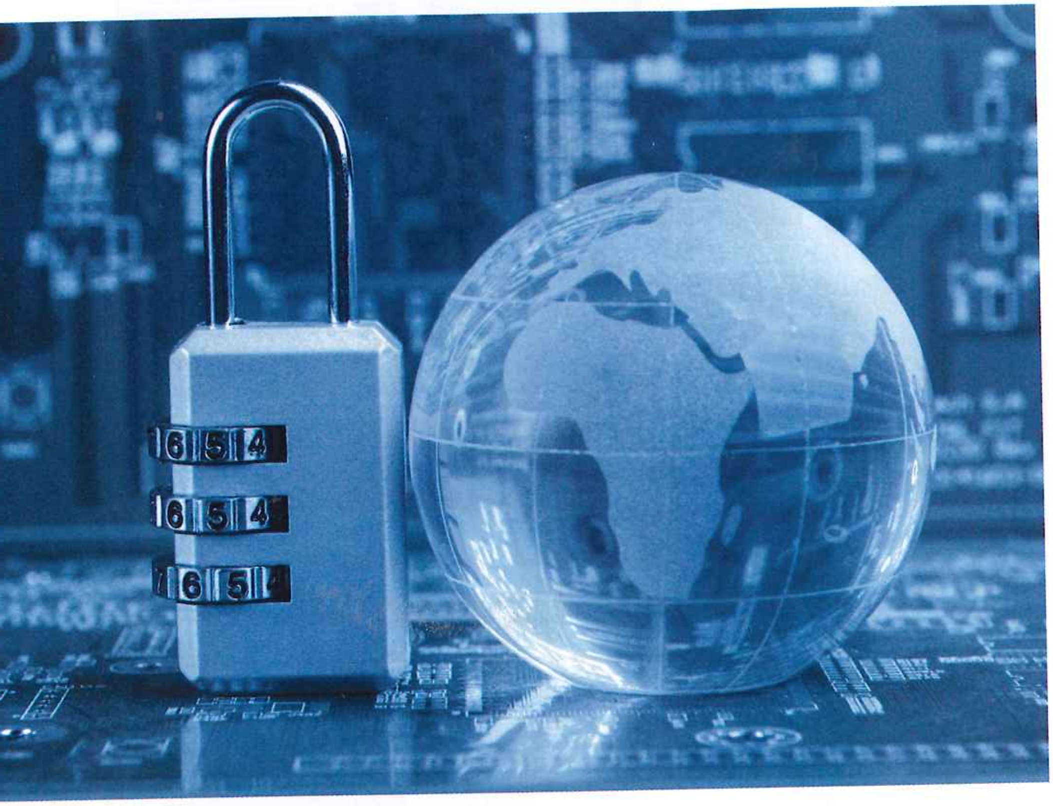
M&T BANK'S BIG DEAL

The Fighter

LT. GOVERNOR KIM GUADAGNO BRINGS NEW JERSEY'S ECONOMY BACK FROM THE BRINK

{NOVEMBER/DECEMBER 2015} **ENTREPRENEURSHIP** p.38 **TECH** p.40 **SECURITY** p.42

{ Security }



LOCK IT UP

Easy steps to significantly improve your cybersecurity

Michael DeVito

Businesses are increasingly moving towards cloud-based platforms for their operational and financial systems. Many companies also allow their employees to work remotely through some sort of virtual private network. While these decentralized, virtual systems can reduce costs related to the purchasing and maintenance of physical servers, other hardware, and software, they also increase the risk of fraud and security breaches.

Businesses need to be aware of the security measures necessary to effectively safeguard this information, many of which are not costly, and devote the time and resources to enact them:

STRONGER PASSWORDS — This is a very easy, inexpensive way of enhancing security. The use of alphanumeric passwords that include the use of at least one symbol, and a password of eight or more characters can significantly reduce the risk of unauthorized access. There are many instances where passwords are never updated or only changed with basic type fields that are common and typically the first attempts used by unauthorized users. Users should periodically update their passwords and, of course, not share them with anyone.

Many cloud-based platforms can also be accessed by smartphones and similar devices. These devices also need to have strong passwords to prevent unauthorized access. Smartphones and other tablet-type devices are constantly being targeted for theft. If strong passwords are not used to prevent the use of these devices, data can be compromised.

DATA ENCRYPTION — Another strong security measure is having all company computers encrypted. This means having information coded in such a way that only authorized users can read or access it. Encryption insures against the loss or theft of these devices by virtually prohibiting access to their stored data.

CYBER INSURANCE — Companies should also consider obtaining cyber insurance, which can cover them for any financial losses in the event of a breach of security by an unauthorized user. These policies are not expensive and could prove to be insignificant compared to the time and cost if confidential information is obtained by unauthorized users.

There are also other safeguards that companies can use to protect themselves, many of which are listed on the official website of the Department of Homeland Security, including:

- Never click on links in emails or open the attachments. Most legitimate e-mails will not contain attachments.
- Do not give out any personal information. Emails may look legitimate, but in reality are "phishing" for personal information. Phishing is any attempt to acquire confidential or sensitive information, including, but not limited to, passwords, credit card information, etc. under the cover of a trustworthy entity through electronic communication.

There are many aspects of fraud that business owners and companies may be exposed to, both from within the company as well as externally. Being aware of some of the cyber threats that exist can help in safeguarding assets and sensitive information.