Counter Cloud and IoT Security Threats

While ransomware dominates the news, experts warn of increasing security threats involving cloud computing and the Internet of Things (IoT). Until cloud and IoT security catches up with innovation, these exciting technologies offer additional opportunities for cybercriminals. Knowing the threats and how to defend against them will protect your business.

Cloud and IoT Terminology

The 2016 Internet Security Threat Report from Symantec advised caution as businesses implement cloud and IoT technologies. Understanding the dangers will help as you prepare defenses against potential cloud and IoT security threats.

Start with a working knowledge of a few key terms:

- **Cloud Computing** – Working with data and programs that live on the Internet instead of on your computer.
- **Cloud-based Service –** Any paid or free functionality, including popular accounting programs, CRM applications, mobile apps and industry-specific software accessed remotely on the cloud.
- **IoT (Internet of Things)** – The network of various remotely controlled "smart" devices such as routers and security cameras that connect with the internet.

- **Botnet** – A group of internet-connected devices that have been infected by malware and are remotely managed by a criminal "master." The master then uses this "zombie army" to attack another system.
- **DDoS (Distributed Denial of Service)** – A DDoS attack targets a cloud-based service (perhaps a server or website) with traffic from multiple infected systems (a botnet). Overwhelmed by thousands or millions of hits, access is denied to legitimate users.

Risk-Taking in the Cloud

More companies now take advantage of the many benefits of working in the cloud. For small and mid-size businesses (SMBs), the cloud makes tools available that were previously out of reach to users with limited resources and expertise.

Unfortunately, not all businesses have implemented adequate security measures to protect data in the cloud. For instance, Symantec reported that the average business uses 928 cloud apps. However, most CIOs in those organizations know about only 30-40 of the cloud apps in use.

In addition, users share a large amount of data on the cloud without the knowledge of the IT department. 25% of this data is broadly shared, making often sensitive corporate and customer information widely available.

Lack of proper security measures can expose any business to numerous risks, including data breach, loss of account control or data, denial of service, insider attack and website hacks.

Securing Cloud Data

From trade secrets to customer information and financial data, businesses create an abundance of sensitive information. With so much of that data now stored in the cloud, organizations must take steps to minimize the associated risks.

Cloud Data Security Steps

- Define and enforce clear policies and procedures around the use of cloud applications in your organization.
- Enforce specific policies for storing and sharing data in the cloud.
- Carefully research your cloud services provider(s). Ask about encryption, data center security, server location and audit trails. Know their security reputation.
- Take responsibility for security on your end by ensuring strong passwords on all devices and keeping antivirus software up-to-date.

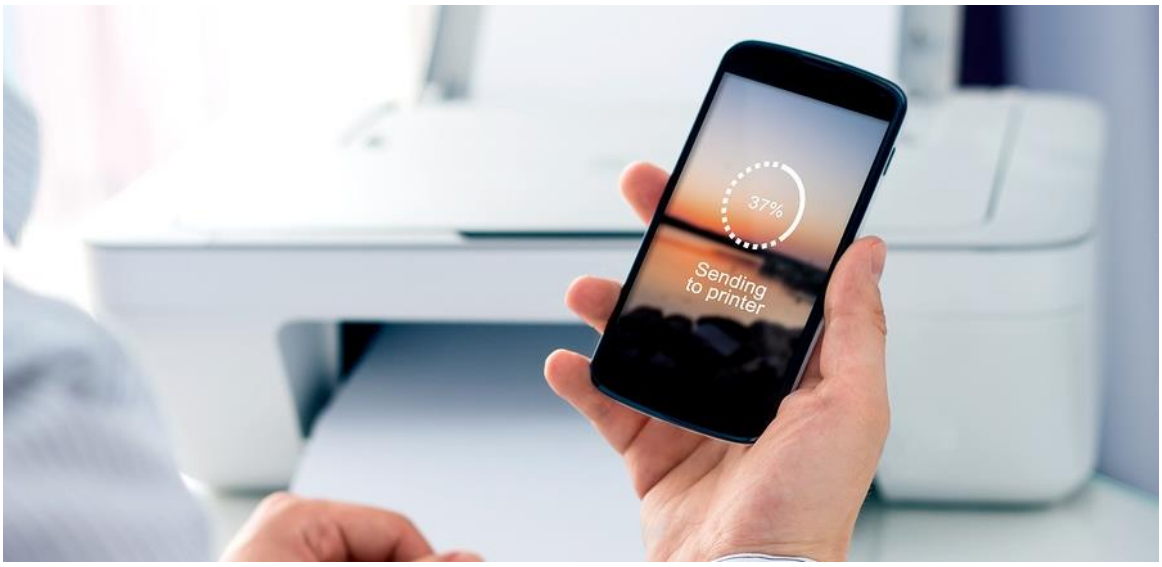
IoT: Business Transformation with a Cost

From security cameras and smart coffee makers, to connected thermostats, asset monitors and printers, businesses already rely heavily on the IoT. These connected devices can increase productivity and reduce operating costs.

Unfortunately, they also present security risks, as DNS company, Dyn learned all too well last fall. In October 2016, amateur hackers created a botnet with 100,000 compromised internet-connected devices.

Infected devices (mostly DVRs and security cameras) launched a DDoS attack on Dyn until its servers could no longer accommodate legitimate traffic. The attack created problems across the U.S., affecting popular sites such as Netflix and Twitter.

The IoT also exposes unsecured businesses to unauthorized network access, identity theft, and application hijacking, as well as botnet infection.



Addressing IoT Security Threats

As you reap the benefits of connected devices, make certain to pay attention to security. For instance, Symantec reported that an astonishing number of usernames and passwords on IoT devices are never changed from the default. This leads to an easily exploited vulnerability.

Basic IoT security steps:

- Audit the IoT devices on your network.
- Use strong passwords for your devices and networks.
- Know the security features of IoT devices before purchase. Modify the default privacy and security settings to meet your needs.
- Apply firmware updates on your devices as they become available.
- Disable remote access if an IoT device does not need it.

Embrace Technology Mindfully

With cybercriminals making headlines, SMBs may hesitate to move to the cloud or implement connected IoT devices. In most cases the benefits of these technologies outweigh the dangers. However, organizations should proceed carefully, making sure that business practices keep pace with technology adoption.

Many providers offer managed IT services, cloud services and technology infrastructure to help business move forward with confidence. Whether you need assistance migrating to the cloud, managing network devices or customized data security, certified network and security experts work with you to ensure a stress-free process.