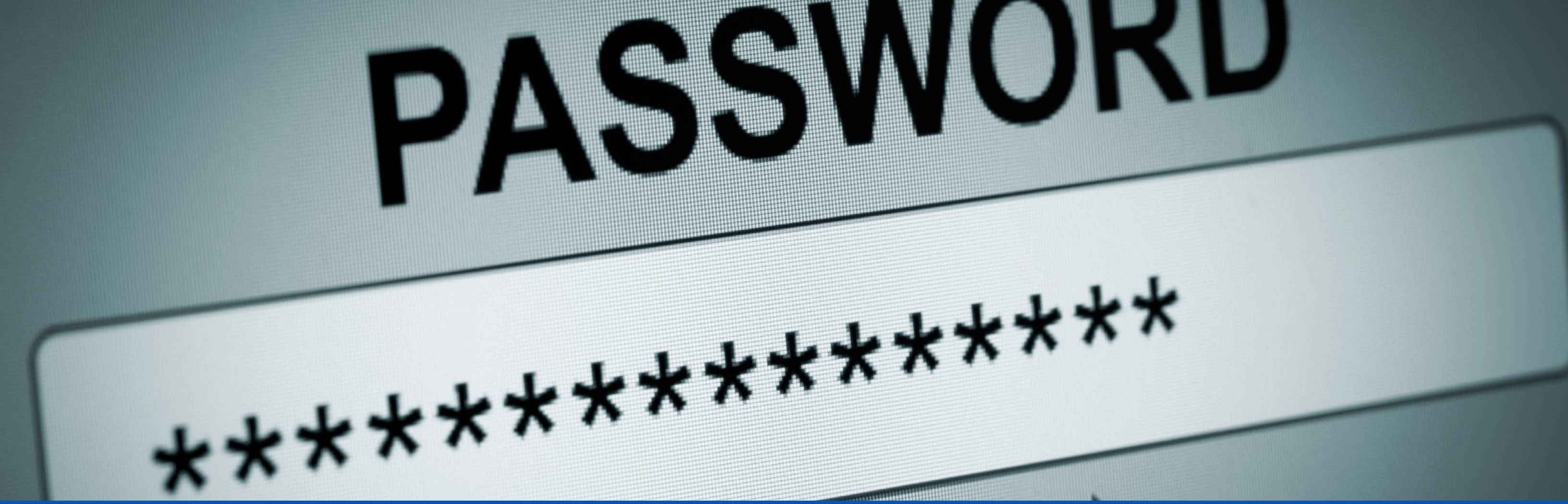


IT for the C-Suite - Quick Read Series
Modern Business Technology Education for the C-Level Executive

By David Moorman - President, DynaSis

Cyber Security Threats of 2018

Cybercrime has been among the biggest headlines in recent years, but with so much other news out there competing for space, it seems that daily run-of the mill tech news is slipping “below the fold”. Don’t be fooled into thinking it’s gone away. Below we look at current trends and the things you need to know.

Ransomware

Yes, the big news, like Facebook’s problems, make the news, but the reports of the continued rise of incidents of ransomware are hard to find. The reality, however, is that ransomware is very much alive and the perpetrators continue to get smarter and smarter.

While we won’t have full data on the effects for ransomware in 2017 for a little while. We can tell you that it continued its trend of record growth. Consider this:

> **Ransomware attacks against individuals:**
> 2017 Q1 – 1 every 20 seconds

> **Ransomware attacks against individuals:**
> 2017 Q2 – 1 every 10 seconds

> **Ransomware attacks against businesses:**
> 2017 Q1 – 1 every 2 minutes

> **Ransomware attacks against businesses:**
> 2017 Q2 – 1 every 40 seconds

Ransomware continues to be a very profitable business for thieves, including those with little experience. The tools a would be criminal needs to be successful are readily available at very low prices (see section below). Companies and individuals can take major steps towards protecting themselves with proper backup and encryption protocols, often best supplied by a managed IT support provider.

Expertise

As time goes by, and as technology becomes more complex, it becomes even more difficult for the small to mid-sized business to keep fully up to date on the wide variety of threats against them, as well as the latest tools available for protecting themselves. Lack of an understanding of how to protect themselves is as big of a threat as the criminals on the attack.

It is critical that any company that lacks the cyber-security knowledge they need for this protection either hire in-house staff that is and remains fully up-to-speed or engage the services of a highly qualified IT support and security provider that can insure your data is secure. An excellent middle of the road approach for companies that have small in-house teams but need security upgrading is a co-sourced (also called co-managed) IT approach where a managed IT service firm is teamed up with the company's in-house team to provide limited services related to cyber security, while the in-house team covers the rest of the company's IT needs.

The Internet of Things (IoT)

You probably already have at least one IoT device in your home and office, and you will have more over time. This may include your Alexa or Amazon Echo device, your doorbell camera, or your smartphone-controlled thermostat. The problem here stems from the fact that these devices create, collect, and store data. For example, during the summer, your thermostat is set to 74 during the day and 72 at night. What is the implication of a hacker seeing that you have reset your thermostat to 78 degrees 24 hours a day? Or a refrigerator door that is opened 30 times a day drops to zero? It is likely that this information can be interpreted to mean that the home-owner is away on vacation, or the business is closed during Christmas week.

The reality is that not enough time and money has been spent on securing the data collected by these devices and as they exponentially increase in number, and as criminals gain more expertise, it becomes more likely that they will become the root cause of an increase in home and office break-ins. The problem is magnified because these devices do not run on software that can be upgraded through regular downloads. They run on firmware (somewhere between hardware and software) that is factory installed without the capacity for upgrading.

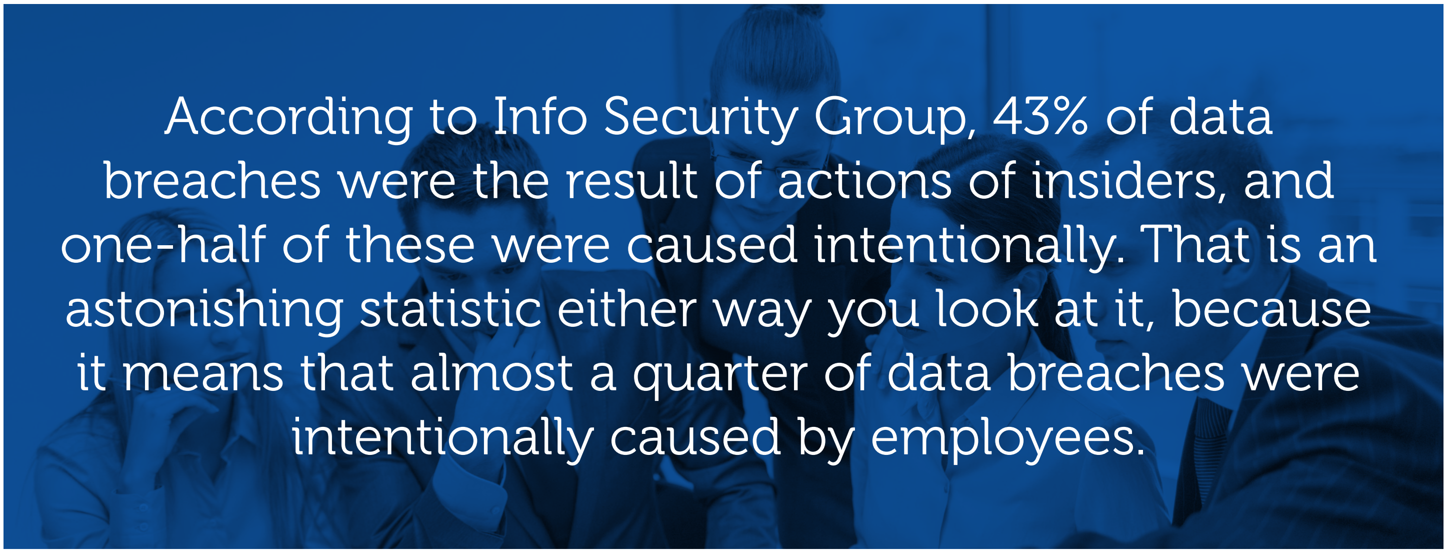
Until manufacturers deal with this vulnerability, consumers and business owners need to be aware that the conveniences for which they purchased certain appliances, may come with unexpected surprises.

Phishing

Hopefully no one reading this article ever fell for the plea from the Nigerian prince to help him save his family's $500,000,000 fortune, for which he will compensate you with the paltry fee of $10,000,000. Or the fake email from the IRS demanding a call to their office to provide them with your bank account and routing numbers to pay your fine or risk losing your house.

But today's cyber-criminal has perfected this "skill" to the point where employees can receive fake emails that look like they come from their supervisors and ask for sensitive information. They also send out emails that look like they come from your bank asking you to change your passwords. The fakes are essentially perfect. Except that at the same time you are changing your password, it is being harvested by the perpetrators and your account will soon be drained. If this happens to a business, sensitive data may be stolen or ransomware may be installed.

Unwitting employee error is the number one cause of attacks on small to mid-size businesses but this can often be prevented through training. A good training program will be ongoing and reinforce your team's preventative knowledge on a regular basis. (Speak with us here at DynaSis about our in-house employee training programs.)



According to Info Security Group, 43% of data breaches were the result of actions of insiders, and one-half of these were caused intentionally. That is an astonishing statistic either way you look at it, because it means that almost a quarter of data breaches were intentionally caused by employees.

Ineffective Passwords

Believe it or not, the most commonly used password is still 123456. People want to simplify things, and that is understandable, but 123456? Really? Think about this: millions and millions of consumer records have been hacked. 87,000,000 on Facebook alone. The hackers can find out your birthdate, your children's names, your pets' names, your nicknames, where you live, where you were born, etc. Their algorithms can take this information and with little trouble, test millions of potential passwords using this information until they break through.

As a business owner, there are at least two things you can do. The first is multi-factor authentication, which uses more than one "factor" to prevent break-ins. The second is to teach your employees about better use of passwords. We used to believe that the use of special characters (!@#$%^&*) was the answer, along with numbers (123456789), but these are limited in number and with the ability to test millions of combinations, the hacker can patiently wait until the right combo gets through. Today, security experts are suggesting combining three or more totally unrelated (and meaningless) words: rabbitscrewdrivercactus, steamboatdinosaurfloating,disposablerestorationfoot. Weird, yes. Long, yes. Easy to remember, yes. Easy to steal, no.

Internal Attacks

The above section raises an interesting point: if it is possible for outsiders to gain access to a company's IT network by deceiving one or more employees of that organization, isn't it also possible for people working for that company to **intentionally** cause similar problems on their own? Of course, it is. Consider this: according to Info Security Group, 43% of data breaches were the result of actions of insiders, and one-half of these were caused intentionally. That is an astonishing statistic either way you look at it, because it means that almost a quarter of data breaches were intentionally caused by employees.

Regardless of their reasoning, whether for personal gain, or disgruntlement, the results can be devastating. The next question is: who are they attacking? While in the early days, they were going after educational institutions, then medical records, today, the majority of these insider attacks are against businesses. The chart below shows that in every sector, except one, percentage of attacks are falling. That one sector is business.

While we are not proposing witch hunts and wild accusations, we do encourage all small businesses to be fully aware. Be particularly aware of disgruntled employees who may have an inkling that their days with your company may be drawing to a close. Also, be particularly vigilant in de-activating access of employees you are terminating before you give them the news.

Hacking Tools on Sale – Cheap

While you may not find them on Amazon, the tools needed for hacking and creating havoc through ransomware and other cyber-intrusion gems are easily available to any would-be hacker who takes a little time to search them out. At one time, becoming a cyber-criminal took real dedication. Software had to be created and the whole process developed from scratch. This took time, money, and thorough knowledge of what they were doing. Today, for a couple hundred dollars, the software needed to attack your company can be bought online. Some of the sellers even have help desks! The problems for you can appear on several levels. Of course, there is the threat of ransomware and having to pay to have your locked files released, as well as stolen records of your customers, patients, staff, etc. But there is another unfortunate possibility, one which we have first-hand knowledge.

We received a call from a company whose files had been totally locked (including their backups which had been improperly created). They received and agreed to pay an $8,000 ransom. Unfortunately, the criminal involved was apparently an amateur who did not know how to use his newly purchased hacking software to release the locked files. We were called in AFTER the fact and engaged two different cyber-forensic companies to unlock the files. Neither could do it and the company lost years and years of client files. All this could have been prevented with some basic security techniques.

The Answer:

Cyber-security today needs to be a multi-pronged effort lead by experienced professionals. Most small to mid-sized companies, even those with small in-house IT departments, don't have the expertise, which needs to be updated on a very regular basis to keep up with latest trends.

At **DynaSis**, we have been helping companies like yours monitor, manage and maintain IT networks including cyber-security since 1992. Give us a call at 678-373-0716.