# Now more than ever

# It's time to invest in cybersecurity

*Cybersecurity for Small and Medium Businesses*

# **White** Paper

Cloud | Cognitive | Cybersecurity

## Excuses, Excuses

“We are too small to be a target.” “We are not regulated.” “We passed our audit with flying colors.” “We don’t have anything a hacker would want.”

These are typical reasons CEOs, CFOs, and even IT professionals routinely give regarding why they are unwilling to invest in cybersecurity.

As cybercrime grows, criminals have profited an estimated $600 billion in 2016 and attackers are successfully infiltrating smaller targets in ever increasing numbers. Cybercrime can have a devastating effect on small and medium businesses (SMB). However, even with a small budget, these businesses can still protect themselves.

It is important to realize there is no magic bullet that offers 100% protection, but with the correct combination of people, process, and technology, a company can ensure that it will not be an easy target.

**Studies show 60% of small businesses that are breached will be out of business within six months. This is a staggering number, but the truth is, most small to medium businesses cannot withstand a significant breach**.[1]

## Are you a target?

The answer is simple: Yes, you are.

In 2012, an HVAC firm was compromised. The firm’s management assumed it was too small to be a target. The attackers did not steal the firm’s data, hold anything for ransom, or do anything to disrupt the day to day operation of the business. All they did was lie in wait.

In 2013, the firm was contracted by a large retail chain in western Pennsylvania to monitor overnight temperatures in the stores in order to reduce the cost of temperature control. The task required remote access to Target’s network. At this point, the attackers made their move. Through credentials stolen from the HVAC firm, the attackers gained access to Target’s systems. The ability for the attackers to access every POS device in every Target store led to one of the largest data breaches in U.S. history.

In the past, small companies may have been correct believing they are too small to have anything of value to a hacker. This is no longer the case. In the past 12 months, more than 50% of U.S. small businesses have been attacked.[2]

## Your data is more valuable than you think

Do you store or process employees’ or customers’ social security numbers, financial information, personal identifiable information or personal health information? This is data, that if lost, could be valuable to a hacker or punishable by a regulator. Just because you are not a Fortune 500 company with a zettabyte of data, that does not mean you do not have valuable information.

The rise of ransomware has also changed the value of your data. What would happen to your business if your employees could no longer utilize the applications and data they need to go about their day to day functions? Ransomware encrypts your data and holds it hostage until a payment is made. If your data is important enough that you cannot do business without it, then that data is valuable to a hacker.

## But I passed an audit

Even after passing their audits, the following businesses were breached: Target, Yahoo, and Dyn, as well as most banks, healthcare companies, and retail businesses.

Passing an audit does not equate with being secure. Auditors look at things from a compliance standpoint not a criminal standpoint. Successfully checking off boxes on a regulator’s clipboard does not mean you are protected. You may have a firewall, but is it configured correctly? You have great security tools, but are they being utilized properly and integrated with internal business processes? When was the last time you ran a health check on your systems?

## What will a breach cost me?

The cost of a breach can be measured in multiple ways. The most obvious is financial. According to Ponemon Institute, as of 2016 the cost of a breach is $141 per record.[3] Ransomware attacks are growing aggressively, up to 6000% year over year, and increasingly targeting the SMB market. This could result in a devastating financial impact.[4]

Loss of cash is not the only way a breach can affect your business. In any business, your reputation is paramount. Companies as large as Target, while disrupted, have survived a breach. However, most SMBs cannot do the same. **I think it is worth mentioning again, studies show 60% of small businesses that are breached will be out of business within six months.**

Additionally, attackers are often after something other than money. Hacktivist groups are not in the game for financial gain, but rather to disrupt organizations which conflict with their philosophical or political positions. One of the more infamous of these hacktivist groups is Anonymous. Anonymous has attacked Sarah Palin's email, the Oregon Tea Party, the Westboro Baptist Church, and scores of other foreign and domestic government officials with whom they disagree. A popular animal rights group is also thought to have a hacktivist arm.

## What can I do?

Much can be done to improve your security posture without the use of major resources. With simple policy and procedural changes, an organization can close a lot of loopholes. One example is limiting local admin rights on end user computers. Without local admin rights, it is much more difficult for an attacker to escalate to the heart of your network. This is a major change that will not cost any money and is an easy fix for your IT team to make. What is more difficult is creating a cultural change within your organization.

### End User Security Awareness

An inexpensive method to increase cybersecurity is to increase awareness among your end users with ongoing training. There are many affordable web based training platforms that can be very effective. Most are customizable based on industry, compliance, and knowledge. In today's world, employees are moving in and out of jobs faster than ever before.

An easy to use, repeatable, and trackable training system is a great way to keep security top of mind. Your employees do not need to become cybersecurity experts, but they do need to think before clicking a link or giving their password over the phone to someone who claims to be doing a project for the IT director.

### Perform a Security Assessment

Performing a security assessment will go a long way toward understanding your security weaknesses. By simulating a malicious attack from either outsiders or insiders, a security assessment with a penetration test can provide an active analysis of your systems and help you proactively protect your information assets and your people from security threats.

### Social Engineering Exposure Services

Social engineering should also be included in the security assessment. Social engineering is defined as the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. In this situation, hackers will use personal or professional information about your company and employees to gain access to a building or to personal passwords. These services are paramount to understanding where vulnerabilities lie in your systems and procedures.

> **"Essextec has a 45-50% success ratio with phishing exercises and 75-80% success rate with phone-based social engineering exercises. Regardless of technical controls in place, the human factor (or Layer 8 issue) will always be the easiest method of compromising an organization."**
>
> Sean Colicchio, Essextec VP of Information Security

## Conclusion

In closing, the most important step any organization can take to ensure its security is to create a security-minded culture. This must come from the top and work its way down to every employee. Simple steps such as the ones discussed here will work only if you have buy-in from the top and the end users accept that changes are made to protect the company as a whole and them as individuals.

REFERENCES:

1 http://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/

2. https://www.cnbc.com/2017/04/05/congress-addresses-cyberwar-on-small-business-14-million-hacked.html

3. https://keepersecurity.com/assets/pdf/The_2016_State_of_SMB_Cybersecurity_Research_by_Keeper_and_Ponemon.pdf

4. http://invenioit.com/security/ransomware-statistics-2016/

For more information on these services or any Essextec Cloud, Cognitive, and Cybersecurity solutions, contact your Client Executive, email us at exceed@essextec, or call 1-888-519-1518

Essextec is an award winning, innovative firm with intellectually curious and highly skilled teams. They help organizations solve their significant challenges by applying innovative Cloud, Cognitive, and Cybersecurity technologies. Essextec consistently enables their clients to exceed their goals and objectives ensuring long-term success.

essextec
A CONVERGE COMPANY

IBM
Platinum
Business Partner