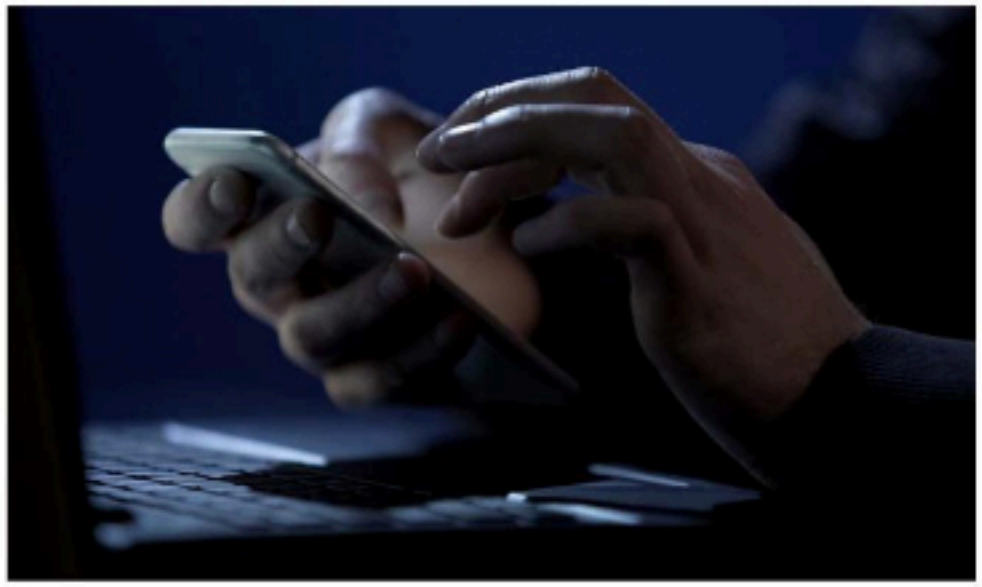
How Can A Small Business Keep Its Data Secure In 2018?

Xac Dinsmore
COO, COMPUTER TECHNOLOGY SOLUTIONS

There seems to be a new data breach, vulnerability, ransomware, or IT related lawsuit nearly every day. How can a small business keep up with this constantly changing landscape? The cloud has introduced some convenience, and even cost savings, but it has also introduced new security challenges. While this is by no means a comprehensive or complete guide to addressing every possible security threat, there are some standard practices that address most of them. It is a minefield out there, let's see what we can do about it.



Before we can discuss solutions, we must first discuss where these threats come from. Some of the most common paths to data loss are email, malicious web-sites, phishing (tricking users into releasing credentials, money, or confidential information), and security vulnerabilities in servers, computers, and network equipment. Another often overlooked threat is physical security, such as locks and cameras. A breach in any of these areas can lead to the release or loss of important data, which can pose both a financial and legal threat to your company.

> "While products are important, your users are your biggest threat. Fortunately, there are some things you can do to help. Password complexity and rotation policies are important, though not perfect. Passwords can still be compromised, even if they are strong and frequently changed. Multi-factor authentication is a simple solution to this problem, and should be used on any internet accessible resources."

The first item, and probably the one you hear the most about, is on the product and software side. Data security involves multiple layers of defense, as no one product is perfect or impenetrable. A firewall should be considered your first line of defense. However, a firewall that is out of date, misconfigured, expired, or insufficiently licensed, may provide little or no security protection. Antivirus (AV) software with behavioral analysis is your next layer. Modern AV programs do more than just look to a list of known viruses and try to stop them. They will analyze the behavior of the system to identify things that act like malicious software, even if it has never been seen before. The AV that comes free with Microsoft Windows has come a long way, but it has no centralized management or reporting features to allow you to identify the who, what, when, where, and how of threats that have come into your organization. While many AV programs and firewalls can do a lot to protect people from malicious emails, a dedicated mail security system is also recommended. Such systems will block known spammers, malicious links, and infected attachments. Keeping these emails out of the inbox is a lot better than hoping to stop them if someone clicks on it. The final, and in some ways, most important layer, is backups. If all else fails, and you are compromised, with good backups you will be able to get your business up and running in short order. Hybrid backup solutions are strongly recommended as cloud only or local only backups both come with drawbacks. A local only backup does not protect you from loss of data due to physical theft, fire, tornado, plumbing leak, or some other environmental factor. Cloud only backups tend to be slow to restore from, causing unnecessary downtime if you need to recover your data. Ideally, your backups run to a local destination first, and then get replicated to the cloud for both high speed access, and protection from environmental factors. If you primarily store your data in the cloud, backups are still of importance, though the approach may be different.

While products are important, your users are your biggest threat. Fortunately, there are some things you can do to help. Password complexity and rotation policies are important, though not perfect. Passwords can still be compromised, even if they are strong and frequently changed. Multi-factor authentication is a simple solution to this problem, and should be used on any internet accessible resources. Multi-factor authentication can work in a number of ways, but typically it will require a combination of a password, and some other credential such as a code from a text message, a smartcard, or an app on a cell phone. This means that even if a password falls into the wrong hands, the account will not be compromised. The next step is to use the principle of least privilege. This simply means that all users should only have the minimum access required to do their job. Following this principle protects you if a user's account is compromised, but it can also protect you from a disgruntled employee trying to do damage to your business. Lastly, user training is critical. It may seem intimidating to train your users in information security, but there are programs out there designed specifically for this. Through these platforms you can send your users fake malicious emails and see how many click on them, or enter their credentials. Training can then be geared towards your staff depending on the results. Videos and interactive games are also available to help with this. A well-educated staff goes a long way towards protecting the interests of your business.

All of this may seem a little daunting, but it really comes down to this. Make sure you have a proper firewall, antivirus, email security, and backups. An expert should implement these products for you as misconfiguration can be worse than not having it at all. Additionally, your users should have strong passwords and multi-factor authentication to protect their accounts, and they should be regularly trained to identify and avoid potential threats. Keeping up on updates for servers, computers, and network equipment is also important. While this is not everything to look out for, if you follow these steps, you should be able to sleep at night knowing that your data is safe.

Xac Dinsmore lives with his wife and two daughters in North Mankato. He was born and raised in the community and is Chief Operating Officer at Computer Technology Solutions on Belgrade Avenue.