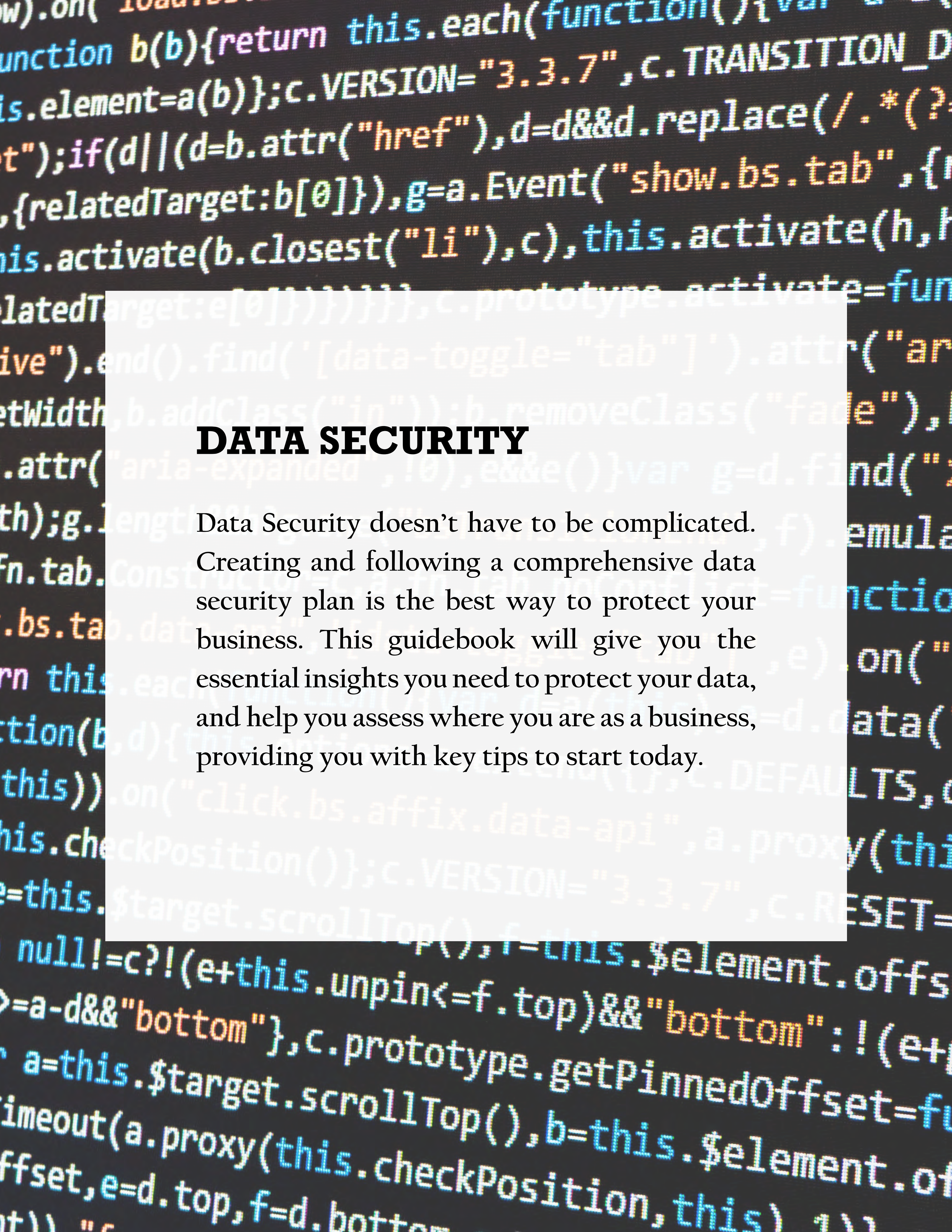
DATA SECURITY
10 Ways to Protect Your Business

Xlingshot

DENVER
METRO
CHAMBER
OF COMMERCE



DATA SECURITY

Data Security doesn't have to be complicated. Creating and following a comprehensive data security plan is the best way to protect your business. This guidebook will give you the essential insights you need to protect your data, and help you assess where you are as a business, providing you with key tips to start today.

10

KNOW THE COSTS

NOT ALL DATA SECURITY NEEDS ARE THE SAME. Before selecting a solution, it's important to understand the risks and financial costs to your business if you lose data or your systems go down. How you calculate this depends on your business model, but some items to consider include:

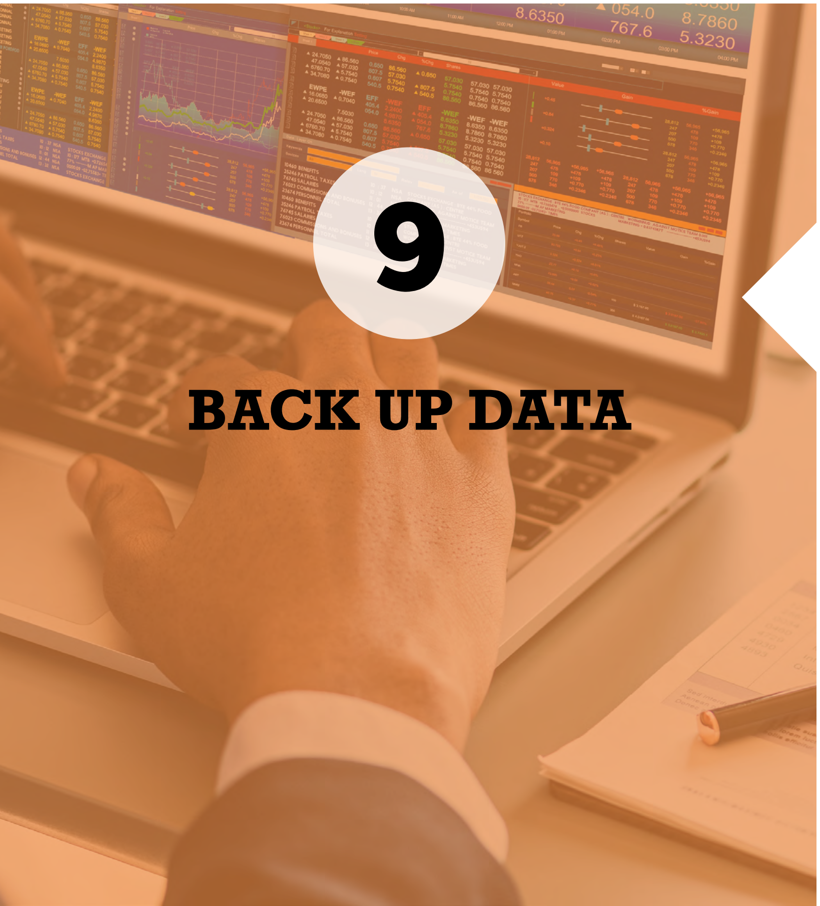
- How many work hours would it take to recreate your data of customer information, billing, vendor information, contacts, etc.? (Would this be possible?)

- What is the total revenue you generate per business hour? (Typically this would be annual revenue divided by 52 divided by 40 but will vary based on your business.)

- For every hour you are down, how much of this lost revenue is recoverable?

- What would it cost you in overtime to recover and catch up for time lost? What other operating costs might be impacted due to lost time?

Running some quick math will help you assess how much your data is worth and the cost to manually recover the information.



9

BACK UP DATA

YOUR BUSINESS CHANGES BY THE MINUTE. Backing up your data only once per day or just weekly doesn't put you in the right position for a fast recovery in the event of data loss. Imagine paying all your team members for the time it would take to reenter information entered in the last day or week. And that is assuming they can recall all the information. Backing up your data multiple times per day provides you with the protection you need and reduces the time required to get back up and running. You may also consider implementing a disaster recovery device that will be immediately ready-to-relaunch with your full system, applications and data to take your recovery time down from hours to minutes.

8

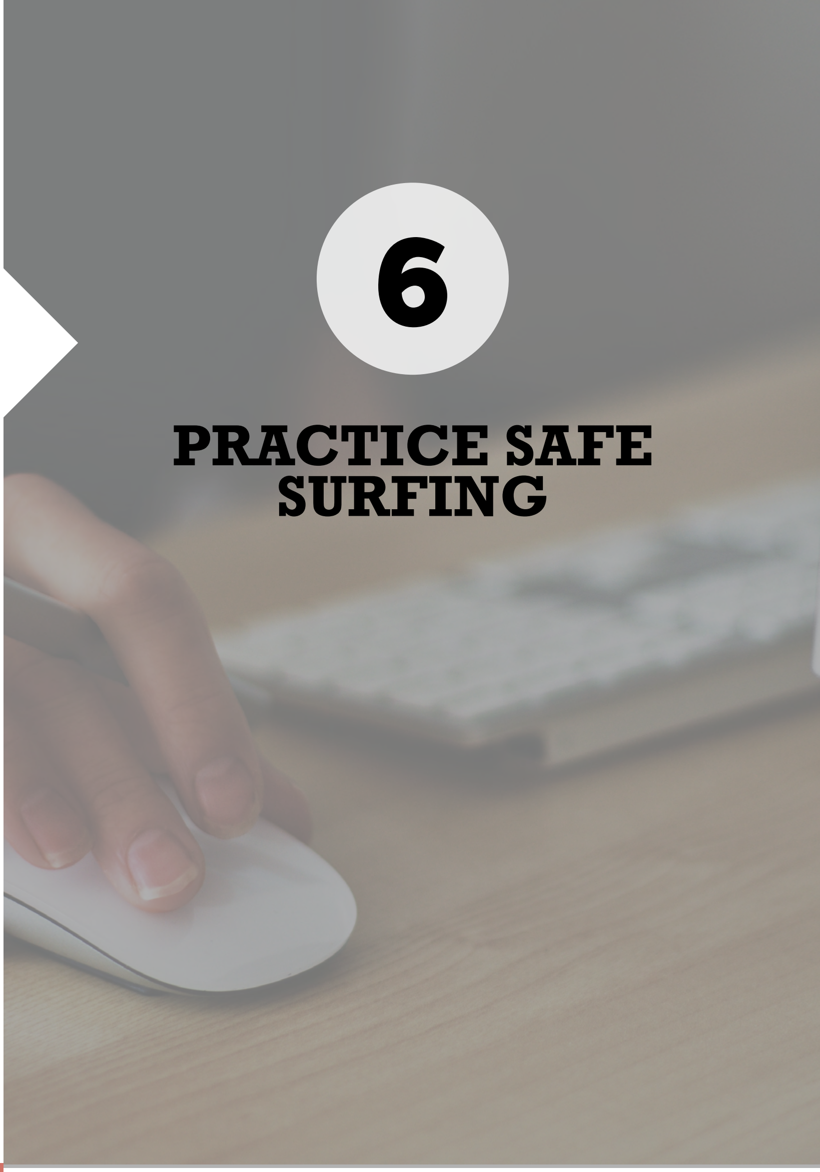
SECURE YOUR EMAIL

ONE OF THE EASIEST WAYS FOR HACKERS to gain access to systems is via email. You need to protect your organization from spam, email-born viruses, email-based malware, phishing emails, malicious links, unsecured email and denial of service attacks. By using solutions that provide advanced threat detection, you can put in place a vital security layer that scans email attachments and compares them against a cryptographic hash database. Emails found to contain malicious content are quarantined and administrators and users can be notified. If no malicious content is found, the email is passed through seamlessly to the user.

7

ENCRYPT YOUR DATA

ENCRYPTION WILL HELP PROTECT YOUR data and personal information as it is traveling through the Internet. For example, if you are passing secure information such as credit card numbers, social security numbers, medical information or even just customer names and addresses, encryption can ensure this data is sent securely rather than as "clear text," which can be read by anyone. Data encryption for your email traffic is no longer an expensive and out-of-reach solution for small and mid-sized businesses. This technology is now available at an affordable price, and can help ensure sensitive data sent over email will safely reach its destination without being "read" by hackers who will use the information for phishing schemes; information gathering including passwords and sensitive financial information; and confidential, personally identifiable customer information.



6

PRACTICE SAFE SURFING

ONE OF THE OLDEST (AND STILL MOST popular) ways of breaching your systems is done via code that is activated when a user clicks on (or in some cases even hovers over) a malicious link. Malware and ransomware can then be quickly installed on the device and your data can be held hostage. While a back-up system can help in this situation, allowing you to recover your data without paying the exorbitant ransom fee, is even better if you can pro-actively prevent the malicious code from entering your system in the first place. It costs a lot less to stop the infection before it starts than to recover from an infection. You also need to have a technology layer in place that checks every data request that is being made out to the Internet to ensure that the requested site is safe. Those which are safe have traffic routed without interruption. Internet traffic to and from sites that include malicious content are blocked. And those that are considered questionable are sent through another layer of security with malware and anti-virus tools to confirm whether they are safe. In addition to filtering data requests, you may want to restrict the websites that your employees can visit. This not only helps to protect your system from malware, it can also help reduce legal liability by preventing access to inappropriate websites.

5

CHANGE PASSWORDS FREQUENTLY

THIS SHOULD GO WITHOUT SAYING, yet passwords are still a problem for many organizations. While it's convenient for users to keep the same password for months or even years, frequently changing passwords can help protect your organization. Here's why: Hackers will often "revisit" and re-use the same account information over and over to continue to access your systems over time. Frequent changing of your password prevents this repeated abuse. Also, if the user's computer is moved to a different employee or it leaves your company (through a sale, theft or recycling) there may be saved passwords stored in the machine. Changing passwords regularly will reduce the likelihood that these saved passwords will still be valid and can help prevent unauthorized access. Tracking that employees are regularly updating their passwords is an important step and solutions are available to help automate and enforce a password changing policy that is appropriate for your company.

4 WATCH OUT FOR MOBILE DEVICES

WHILE MOBILE DEVICES CAN ADD A LOT OF convenience and productivity for your employees, they also add a lot of risk to your business. That's because mobile devices are often using networks that are not protected by your own firewall. These devices create an additional security risk because typically they are not protected from malware and viruses. But mobile devices can be safe to use if they are set up properly with the right security layers in place. Similar to how you protect your network with technology that filters web traffic to confirm its safety, your mobile devices can be installed with lightweight versions of the same technology. This layer ensures that data requests being made out to the Internet are exchanging information with safe sites. If you have employees on mobile devices that aren't using this additional security layer you may be introducing malware and viruses onto the device and then into your overall network. In addition, we recommend mobile devices be connected only to your "guest" (or separate network) from your default corporate/employee network, creating another security layer between your mobile devices and your core network applications and data. One of the best ways to protect your systems is to remotely delete all data on a mobile device in the event it is lost or stolen. You'll still be out the cost of the hardware, but it can reduce your exposure to the more significant costs of stolen data.

3 TRAIN YOUR EMPLOYEES

IT'S CRITICAL TO TRAIN YOUR EMPLOYEES so they can recognize phishing schemes, malicious links, suspicious emails and sophisticated hackers using social engineering to gain access to your systems and steal your data. This is your number one line of defense, yet is often skipped by small and mid-sized businesses. The best data security system in the world cannot overcome an employee who unwittingly provides access for hackers. Implementing a cybersecurity training program will provide your employees with the critical skills they need to avoid falling victim to hackers, thereby compromising your systems. Employees can be trained to recognize potential dangers and report potential breaks in security. There are a lot of cost-effective training options available today that can be implemented with in-person instruction or flexible and efficient online courses. You can also track your employees' progress as they complete coursework and even test how they are applying their knowledge.

2

DEFEND YOUR NETWORK & TEST REGULARLY

HAVING THE BEST TECHNOLOGY DEFENSE for your systems means having the right protection in place at every layer. Not only do you need to block known threats like ransomware, botnets and phishing, but you need to detect and contain advanced attacks before they can cause damage. Your security needs to go beyond your network, because often your devices are being used remotely on other networks including your employees' homes, airports, hotels, customer sites and those provided by mobile phone carriers. Moving forward with a multilayered approach is essential for a comprehensive protection strategy.

- **Network:** Put in place firewalls with updated patches supporting malware detection and virus blocking

- **VPN:** Set up a Virtual Private Network (VPN) and require employees to use the VPN to access the corporate network when they are working remotely

- **Computers & Mobile Devices:** Install protection on the device itself, regardless of what network is used

- **Cloud:** Ensure you're working with a reputable cloud provider, with extensive physical and technical security layers in place, including encrypted data transmission

- **Email:** Encrypt data and conduct security scans on file attachments

- **Employee Training:** make sure your users have the information they need to successfully ward off intrusion. Once your security system is up and running, test it regularly using automated tools and even fake phishing emails and phone calls to ensure hackers can't penetrate your system.

1

MAKE A PLAN

AND FINALLY, THE NUMBER ONE WAY TO protect your business is to START. Make a plan and start implementing these solutions as soon as possible so you can avoid becoming a victim of sophisticated hackers, natural disasters and user errors that can compromise your data security. For a free data security assessment, please contact Xlingshot today. We can review your systems and help you move forward with a more secure IT approach to secure your data and protect your business.

Xlingshot

xlingshot.com

DENVER
METRO
CHAMBER
OF COMMERCE

denverchamber.org

Call us today for a free consultation or for more information on data security and how to protect your business. Email info@xlingshot.com or call (303) 410-2845.

This guide is intended as a general educational and informational resource. The Denver Metro Chamber of Commerce makes no representations or warranties of any kind, express or implied, about the completeness, accuracy, reliability, suitability or availability with respect to the content of this or any other guides. Any reliance you place on such information is therefore strictly at your own risk. In no event will we be liable for any loss or damage in connection with the use of this guide.