Secure our Small Businesses

and Why We Should All Care

William Gates  
Cybersecurity Operations Technician & Engineer  
Colorado Army National Guard

March 18, 2021

# Abstract

The interest in this topic began several years ago when I witnessed the extent to which a small business in my community was harmed by a relatively minor hack. The company had fewer than 10 employees and many times that number in contractor associations and customer accounts. Their cyber security program began and ended with the ISP’s modem and the technical expertise of a part-time IT enthusiast. Many small businesses don’t have the resources to commit to effective talent. Experienced cybersecurity professionals are expensive to train and pay. The demand alone is contributing to increasing salary offers and benefits only a large corporation can provide. However, for this small business in my community, they got me, an entry level cyber security professional desperate for some real-world experience. Since that engagement, I wanted to find more stories involving small businesses who were impacted by a cybersecurity experience. I listened to one that ended in the worst possible way, going completely under.

The goal of this whitepaper is to discuss how a significant effort to secure small businesses can make a positive impact on a population’s personal security, professional security, supply chain security, and the 3rd party vendor contract relationship. This paper will also describe and discuss several cost effective and achievable methods improving security and managing risk. The methods discussed are categorized into two pillars of effort, Individual Security and Organizational security.

# Keywords

Security – in the context of this white paper this word encompasses both cybersecurity and physical security domains.

Cybersecurity – refers to security management, operations, techniques, tactics and procedures used to defend, monitor, and manage risk involved with computer network infrastructure, devices, services, and data. This includes the protection of data at rest (storage), data in transit (active communication), and data in use (processing and user interface). The physical protection of people, equipment, and media (e.g. laptops, paper, ethernet cable, DVDs, USB devices, printers, web servers, routers & switches, etc.) is a critical component.

# Acknowledgements

This white paper could not have succeeded without its contributors who provided additional research, peer review, and editing.

Table of Contents

[Abstract 2](#_Toc67015718)

[Keywords 2](#_Toc67015719)

[Acknowledgements 2](#_Toc67015720)

[Introduction 2](#_Toc67015721)

[Individual Security 4](#_Toc67015722)

[Methods 4](#_Toc67015723)

# Introduction

To understand why cyber security even exists, it may be helpful to understand the nature of the internet and how benefiting from its many advantages cannot exist without accepting all the disadvantages. In other words, the internet “good” cannot exist without “evil” or the internet “light” cannot exist without “darkness.” Kind of like the philosophical debates posing that darkness cannot exist without light because darkness depends on the absence of light. Also, my theory that good cannot exist without evil because good needs something to measure against. Good is relative to morals and values what we perceive to be less than good or not good.

The internet was not originally designed with security in mind. Before it was even called the internet it was a small network connecting university and government mainframe computers together. Over time the network expanded to include more universities. Private networks not connected to this early internet were created by some business to improve the sharing of data internally. With the increased usage of the internet many wanted to connect these isolated island networks to the greater global internet. Then the personal computer was invented making it possible to access the internet from your home. Applications like email and websites were developed increasing communication and the sharing of ideas which soon led to its business advantages.

----------------------------------------UNORGANIZED IDEAS BELOW THIS LINE----------------------------------------

The legal consequences and financial impact of a hack or stolen data is more difficult to recover from and small business is typically low hanging fruit caused by limited resources available for security.

The government (specifically the DoD in my experience) allows for outsourcing and has regulations designed to benefit small, veteran owned, female owned, minority owned companies. The rules are designed to give the disadvantaged a fighting chance to succeed but also has the unintended consequence of creating a bigger attack or intel exposure, a “steppingstone” leading to the bigger primary target. Yes, there are policies and audit programs in place to require vendor and contractor compliance, but enforcement isn’t 100% effective and relies heavily on human behavior. Additionally, most mitigations are “check the box” items that may say compliance was achieved, but real effective compliance is difficult to ensure.

Big business also benefits from small companies and employees that understand and practice good cyber security practices. There are many cases in the news that highlight the threat a 3rd party vendor can introduce to another company.

Malicious or bad actors are constantly scanning the internet to find devices exposed to the internet. This is occurring so much that its often referred to as the white noise or background noise. It’s always there much like the cosmic radiation background is always observed by astrophysicists. Shodan… UPnP…

# Individual Security

Educating and promoting security best practices for individuals within your company is critical to the success of any organization’s security program. People are the most important asset of any organization and pose the biggest cybersecurity risk. Humans are not perfect and make mistakes and therefore can be tricked by other humans.

## Methods

1. Complete an inventory of your internet life. Save all your credentials in a reputable password manager. I have been using one for a few years now and I cannot imagine my life before it!
2. Implement two-factor authentication for every account that allows it. If you are a cyber conscious self-proclaimed nerd with a chip on his shoulder and want to help the security of the world at large because you have or want to have a good heart, you can just send a brief email to all the companies that do not allow this and ask why.
3. Opt-out of email subscriptions and telemarketing. Never unsubscribe from the link in the email. Use your favorite browser (DuckDuckGo or Firefox are my favorite at the time of this writing) to find the company website and research their unsubscribe or opt-out of communication procedures.
4. Make sure all your passwords are different and randomly generated. Use your favorite reputable password manager application. Especially accounts used for your financial and business-related services.
5. Request that your unused accounts are deleted along with all your data. Reputable companies should have procedures documented for doing this. If you cannot find it, email the company until you get an answer.
6. Create a proxy phone number. Create a personal professional email. Do not use your name in the address and at the same time keep the name classy and professional. Use it for your financial or personal professional accounts.
7. Do a privacy, security, and content review of your social media presence. Advertisement driven companies sell your data and read your content and email. This includes Google, Facebook, Instagram, Twitter, Tik Tok, etc.

* Remove people who are not really your friends, family, or colleagues.
* Create a separate social media account or group if you are a public figure.
* The company your work for will read your content.
* Reduce your Gmail usage. Protonmail for the most security or use Apple and Microsoft email services just to have a company that does not sell your data.
* Keep current or future background check requirements in the front of your mind when doing this. Everything public or open source is fair game.

1. Periodical Audits. Inventory your internet life periodically. Yes, it’s time consuming but with a simple calendar reminder you can achieve this. I recommend annually at a minimum. At the same time, audit the passwords you use and change those increased risk of compromise type accounts like email and social media. Credit Check audit.
2. Keep your work and personal life isolated the best you can. If you can afford it, have separate computers, and separate networks at home. There is no reason why you should not have separate email accounts.
3. Network isolation. In this white paper I have cost effective examples of how to do this with minimal network or internet connection downtime.
4. Mobile Apps. Delete unused apps and review what they can access. Pay attention to what country the app was developed in. In this white paper I talk about methods for accomplishing these. Include this in your periodic audit.
5. Hold companies you share data and do business with accountable for their cyber security posture and incident response practices and policies.
6. Know your internet presence and exposure. I talked about Social Media earlier, but this is more than that… Search for yourself and see what can be found about you on any site. Pretend you are an FBI agent and find the smallest of connections that could be added up to form the big picture of you. If you have a high security or high security clearance job, pay attention to your private and professional connections. I’m going to sound like a parent here… Don’t associate with criminals or foreigners that you don’t really know or trust. Of course, exceptions can be made if you are a public figure or have a public presence, but you already have a separate internet/social media presence for this. Right?!
7. Use Signal or another reputable company’s application that uses encryption for personal-professional and business communication.
8. Backup your data regularly. Create a routine that is realistic for you to maintain long term. Ransomware vs Loss of Integrity. Offline, cloud, and a hybrid of both backup strategies. Everyone I know has learned this lesson the hard way at least once. Especially if you grew up like me and constantly pushed buttons on the keyboard and mouse to figure out what they did. I was too impatient for instructions. I suppose I still am to a large degree. I just crave getting my hands in it. For better and worse, I learned so much by just pushing buttons and I highly recommend it for you as well! Keep in mind, every mistake can be reversed EXCEPT the loss of data. Yes, there are methods to recover deleted data, but that’s a different subject than what I’m discussing here.
9. National and International Laws and Policies. Consider the laws and policies of the home country of the internet or cloud services you use. Websites, cloud services and storage, etc. I recommend avoiding North Korean, Iranian, Chinese, and Russian companies or multinational companies that associate with them. Is the company in the U.S.? Does that U.S. company store data in a foreign country? Does that country share my values as it relates to privacy and security?