Why Cybersecurity Matters

if

You Want to Do Good and Make Money:

How to Boost Your Bottom Line

by Better Cybersecurity

Philip Lohr

http://smallbizcybersec.com

Table of Contents

Ignoring Cybersecurity is Bad for Your Business

Computer security involves providing protection from adverse situations. Typically, we think of this as being protected from hackers and things hackers do. But security also deals with making sure your systems are running properly. So events such as power surges, equipment failure, problems from poorly written programs, and even human error are things a good security program can address.

When you first got your computer, once it was set up, it probably performed pretty well. Over time, you may have found that it no longer performed like it used to. Why?

Often, it's a matter of an accumulation of extra files and information left over from normal activity, such as visiting lots of web sites. Other times, it may be that additional software has been introduced that conflicts in some way with software already present. Or, that additional software may be poorly designed.

In some cases, you computer may have become infected with malware. (Malware refers to any MALicious softWARE, including viruses, trojans, keyloggers, and other varieties that do things that you don't want to have happening on your computer.)

One of the more recent introductions is something called cryptominers, introduced with the advent of cryptcurrencies such as bitcoin. A lot of processing power is required for bitcoin to work. You may have heard reference to blockchain. Blockchain is basically a system to manage bitcoin or other cryptocurrency transactions. It is based on cryptography and requires a lot of calculation.

In order to get enough processing power, criminals have developed software (cryptominers) which they can place on YOUR computer and then they can use YOUR computer to do all that processing. One of the problems is that it can slow your computer down and make it perform poorly.

Whether it's a crytominer, a trojan, or some other malware, the criminals are breaking into your computer for THEIR advantage, without concern for YOUR interests. A lot of the time, that is harmful to you.

Some of the consequences of this are:

- Slow performance (sometimes even to the point where your computer freezes up completely)
- Your computer may perform erratically
- Some of your programs may no longer work

- Your data may be stolen
- Your customers' data may be stolen
- Your data may be altered or corrupted. As a business, you rely on your data to be accurate.

There are other consequences. One of these is higher costs. This includes the cost you have to pay to fix the problems. It also includes the cost of wages for the extra time it takes for your employees to accomplish their work. Revenue may decrease because less work is getting done because the computers are slow or are "down."

It may include a higher cost of customers support due to the problems caused. This could be because your slow computer is slowing down customer service, or because it takes longer to deliver products or services. Delays or failures such as these can result in lost or dissatisfied customers.

Small problems can add up to large costs. If you have a help desk, you have higher support desk costs because of the problems that have arisen. Even something "simple" like resetting forgotten passwords ends up as high support costs. If you don't have a help desk, someone is still having to fix the problems and that typically means you are paying for it, either directly through higher costs, or indirectly by the lost focus and lost time resulting from the need to fix problems when you could be spending time and energy focused on your business.

If your systems are compromised, whether by malware or by a hacker's actions, your data may be stolen or compromised. If your competitors get that data, you may lose a competitive advantage.

Stolen data may include your customers' data. If sensitive customer data is stolen or viewed by someone who shouldn't see it, you have a data breach. Regulations require reporting that and you may be subject to fines and legal action. The direct costs of responding to a data breach can be enough to cripple a business.

When the breach becomes known, your customers aren't going to be happy about that. You will likely lose existing customers. Your reputation is likely to suffer. And many of your potential new customers are likely to steer clear of you. They will probably go to your competitors because they are wary of you and the way you run your business. After all, you don't protect your customer data!

Many cyberattacks target your money. Small businesses are highly targeted for these kinds of attacks, in part because they are less security-conscious and not as well protected.

In addition to attempts to steal your money, many attacks disrupt your systems. They may slow them down, cause erratic performance, disrupt their ability to function, or cause them to stop working altogether. If your systems are not functioning, or are not functioning at a satisfactory level, you cannot function in business. This causes dirsuption to your business, frustration to you and your employees, and higher costs. It can also result in loss of revenue and lost customers.

Imagine a web site that can't be reached by your customers. Or a web site that now runs so slowly that your customers have to wait, and wait, and wait for the page to load. Everybody's in a hurry and even a few seconds of delay may result in them going to a competitor. If the time to load the page runs closer to minutes, you will lose a lot of business.

It's not just web servers that can be impacted this way. Any kind of attack or other security issue that causes your system to run in anything other than an optimal manner can hurt your business.

In addition, if your computer is compromised by an attacker or by malware, it may be used to disseminate hate or propoganda, to attack other systems, to send spam, to con or scam others, to store stolen data or illegal data (such as child porn), or as part of an effort to steal other people's money and data.

This is only a partial list of the consequences of ignoring cybersecurity or doing a poor job with it. The negative impact can be significant. Roughly 60% of small businesses fail within six months of a successful cyberattack.

As illustrated above, even if you don't suffer a significant cyberattack, issues and disruptions from poor security can hurt your business.

Truly, poor or inadequate cybersecurity is bad for business.

Cybersecurity, Your Health, and Your Business

It's been proven that stress has a significant impact on health. While stress is something we can't avoid, there is a great deal that we can do about dealing with it. One of the ways is in how we respond to stress. A second way is by addressing the situations that result in stress and finding solutions to them.

As a business owner, constantly having to "put out fires" when things go wrong can be a major cause of stress. We've talked a little about the kinds of things that go wrong, especially when we don't have a good system of managing our computers and technology, or when problems occur because we haven't done a good job with security.

Even if we can get those issues resolved fairly quickly, it adds to our stress. And dealing with the issues take us away from running our business and serving our customers. If there is a problem that is difficult to solve, our stress levels are far higher.

There is another issue when it comes to cybersecurity. Most people don't understand cybersecurity, or how and why security problems occur, or how to fix those problems or limit their impact, or how to prevent them in the first place. To many, cybersecurity seems hard and somewhat of a mystery.

So, if we hear a news story of the latest wave of ransomware, we worry that we may be its next victim. We have heard of hospitals or community governments that have been hit by ransomware and paid large fees (ransoms) to get their data back. (Ransomware is a type of attack where the data on one's computer is encrypted by malware, rendering it inaccessible. At that point, to get access to that encrypted data, you have to pay a ransom, or lose access to it forever. A foreboding message is usually displayed on the screen telling you this has happened, and how to pay the ransom. If you try to access your files, you will find you can't.) The threat is real and prevalentl

A large percentage of ransomware attacks are directed against small businesses. The threat is real. The impact if you are hit, coupled with the mystery around ransomware itself, can cause anxiety and stress. It is certainly sufficient reason to keep a business owner awake at night. There are steps to protect yourself and to recover without paying the ransom, but only if you take action beforehand.

There are so many unknowns for the entrepreneur and small business owner when it comes to cybersecurity that it could cause one's stress level to go through the ceiling. If is often tempting to ignore it and hope you won't be a victim. Of course, hope is not a good strategy. There are a lot of simple things one can do to protect oneself and one's business, even a very small business. But it means finding out more about the topic and that can be overwhelming unless you have someone to help you navigate the maze.

So, there are the known issues that cause problems with the day-to-day performance of our systems, some due to poor cybersecurity and some due to failure to put in place robust systems to protect our businesses, information, and technology.

Then there are all the unknowns and threats that might hit us. This is fueled by frequent stories of data breaches and of ransomware, other malware, and hacking attacks. Unfortunately, the advice given, even if good, is inadequate to provide protection because it is only a single piece of the puzzle of protection that is necessary.

The consequence of ignoring the issues or of making the wrong choices is frustration and lost sleep at best. At its worst, it includes loss of money, reputation, and customers, or potentially complete failure of the business.

So, if we don't bury our head in the sand, we are likely to experience significant stress when we think about cybersecurity. And, if we do bury our head, at some level we still know that our strategy of avoidance could well come back and bite us badly.

There may be cases where a business owner has not given serious consideration to cybersecurity but is not concerned, and so does not experience the stress I have discussed. But that is a dangerous situation to be in. Swimming in shark-infested waters where there have been recent shark attacks is dangerous even if you are completely ignorant of the presence of the sharks. Doing business in ignorance of the risks from security failures is a similar situation.

Now, if you happen to be in business where you create craft items, which you sell at the flea market on weekends for cash only, without keeping any customer records of any kind and without using computers, cell phones, or other technology, you may be exempt from needing to consider cybersecurity. But most businesses underestimate their risks and are actually swimming with hidden sharks. Most business owners should probably experience more stress than they do, when it comes to known or suspected issues or threats.

How do you behave when you are stressed? Do you find yourself more irritable? Do you handle issues as well as when you are relaxed?

How is your focus and performance when you are stressed? Do you have the same degree of focus as when you are at ease? Or does peak performance become an unattainable goal at that time?

What about when you are losing sleep? Can you think clearly?

Do stress, anxiety, frustration, and lack of sleep allow you to bring your best to your business, to your relationships and the interactions with your customers and business partners? Are you able to be creative to find solutions to problems or to improve your business? Are you able to effectively solve problems?

Or do you find that even the solutions that you normally would apply to the things that arise in the normal course of business can sometimes escape you because you are distracted and your inner resources are at a low?

For many entrepreneurs and small business owners, high levels of stress, loss of sleep, worry, anxiety, and the like may be a frequent experience and may be something you have learned to live with. You can still run your business. But, if you're honest, you will probably admit that you could do better.

What if you could find a way to resolve the issues, to find greater clarity regarding "unknowns," and to find solutions to address the kinds of problems that "might" arise? What if you could gain a way of looking at the realm of systems problems and cybersecurity that could provide answers, and you were able to implement solutions that you KNEW would address most of the issues, including most of the unknowns? Would that help you sleep better at night? Would that alleviate some of the stress? Could you perform better if you were able to accomplish that?

I can tell you that it is possible to do that. At the same time, it will take some work and time. But you can do it. The best way is to find someone that can guide you. If you do it on your own, it will likely take more time than you want to spend and you will experience more frustration and make more mistakes than you want to endure.

Don't ignore implementing systems to help you manage your business. Don't ignore cybersecurity. Put systems in place. Learn a way of understanding the threats, your vulnerabilities, and the best ways to address the risks your business faces. Your health will be better. You will be able to focus on your business, both because of fewer issues and because of being in a more productive and empowered state. Your business will be better.

You are getting this e-book as a gift and have been added to a mailing list at the same time. If you remain subscribed to that list, you will receive information that will be helpful to begin to improve your cybersecurity posture. I encourage you to stay subscribed to the list and to read the e-mails.

Of course, you are welcome to unsubscribe at any time. And there are other resources to help you out there.

If you want to address any cybersecurity concerns at a faster rate, you can contact me to discuss options. I have a simple framework that will empower you to understand and to begin to address cybersecurity concerns. I expect to offer that as a workshop or other training at some point. If there is enough interest, I may do that sooner. I also provide consulting services.

In any event, whether through resources you receive from me by e-mail or online, through personal help from me, or from some other trusted source, my hope is that you will

1) recognize there are reasonable solutions for small businesses, regardless of whether or not you have any technical understanding and

2) begin to take the steps to protect yourself, your information, and your business.

Your health and your business will be the better for it.

Cybersecurity Done Right Is Good for Your Business

Now, let's shift to a picture of cybersecurity done well. Doing cybersecurity well does not mean there will be no problems and that you have no risk whatsoever.

What it does mean is that you have protections in place to handle the most serious threats to your business. It means that you also have plans and procedures in place to address any risks and to reduce the impact of any remaining threats. If an incident does occur, you know that the impact will be limited and that you can handle it with minimal disruption to your business.

Even if an unknown situation arises, you already have plans that will adequately address and handle those situations. How is that possible? By using the right framework to approach cybersecurity and to develop your plan to address possible risks, even unknown ones. The details of that are a subject for a different and more in-depth discussion, one that takes into account your particular circumstances.

When you do that well, you obtain numerous benefits:

You make better decisions about your security spending, choosing solutions that effectively address the risks your business faces. As a result, you get a better return on your security spend. The approach most businesses take is to throw popular solutions at a problem which may or may not be relevant and which usually leave significant gaps in their protection.

A robust, well-designed approach to cybersecurity means fewer problems. That results in lower costs and less disruption to your business because you avoid the problems that occur when you don't take such an approach.

You reduce your stress, because you are confident that you have a good plan that addresses your greatest threats, one that gives you a way to deal with any issues that do occur without significant disruption to your business.

When you do hear news of the latest security threat, you already have a framework to quickly evaluate the likelihood and type of impact it could potentially have on your business. You also understand how the protections you already have in place are already protecting you and, if there is a gap, you have a giant head start on how to address that gap. You don't have to lose sleep worrying anymore. (If you are someone who can ALWAYS find something to worry about, that would be a workshop for my work in psychology and personal development. :)   If that is you, you can now worry about the fact that have to come up with something new to worry about.)

You are able to be more focused on your business with greater access to your creativity, brainstorming, and problem-solving abilities because you are not constantly distracted by the multitude of issues, problems, or worries that occur when you don't have good systems and cyberecurity solutions in place. As a result, you will be more productive. Your improved mental status and reduced worry, frustration, and anxiety will also allow you to be more effective in your relationships with customers, employees, vendors, partners, and prospects, which will have a positive impact upon your business.

You can focus on your business because your attention is not constantly being distracted by emergencies and problems that need to be addressed. Even if someone else is responsible for the details of handling those problems, your awareness of them can be distracting. By eliminating the recurring issues, you can now place your attention more fully on improving your business, considering new revenue streams or strategic partnerships, or ways to deliver better customer service or employee satisfaction and retention. You can brainstorm creative marketing strategies. You can now build your business and make it better, more resilient, and more profitable.

Your business will run more smoothly, because it is no longer being disrupted by nearly as many issues as it previously was. That can only help your business. Your service delivery may also improve because it's not being derailed by issues. That can translate into happier customers and, as a result, more sales.

Good security means you are keeping your customers' data safe. That is not only good business, it is increasingly a requirement of laws that require protection for your customers' sensitive information, which even includes their e-mail addresses. If you do a good job of protecting your customers' data and demonstrate that, they will trust you more. Their confidence in your business may increase and that can result in more revenue.

Your company data is safe. Your employee's personal information is safe. Your proprietary secrets, business plans, financial data, and other information does not fall into the hands of competitors, thieves, or the press.

Your money is safe. Establishing good cybersecurity practices can keep you from losing considerable sums of money from attacks and scams.

Good cybersecurity can keep your computer running efficiently, free of disruption. This does not mean you'll never have any issues, but they will be far less disuptive and more easily handled than those that occur due to poor cybersecurity practices.

Good cybersecurity can keep you from going out of business. As just stated, attacks and other issues that cause poor performance can result in lost customers. Other issues, like data breaches cause loss of customer confidence. Roughly 60% of small businesses fail within six months of a successful cyberattack.

Going through the process of establishing a good cybersecurity plan can give you considerable clarity about your business. It can help you gain understandings and insights, see connections and gaps, and shine the spotlight on risks and issues as well as opportunities that you hadn't considered. All of this clarity can help you fix problems in your business, discover ways to save money, add more revenue, and improve your business in many other ways.

This is by no means an exhaustive list but should help you recognize that cybersecurity is not just a necessary inconvenience or something to put aside until you have more time or resources, but is an essential part of running a profitable, sustainable, and effective business.

Cybersecurity: Doing Good

We have already touched on this, but there is an important additional element. Let's break down "doing good" into 1) the good you do for you, 2) the good you do for your customers and employees, and 3) the good you do for your community and the world.

Doing good for YOU (and your business).

We have already talked about this. You benefit from greater peace of mind, less worry, better sleep, and freedom from fear around what could go wrong or how your business could suffer from cyberattacks or other issues.

You benefit because you have confidence that you are protected and can survive adverse situations because you have a robust plan in place that addresses known and unknown issues.

You are better able to focus on your business because you are not being distracted by the issues that result from poor cybersecurity and inadequate systems.

You have greater clarity about your business, through understanding the framework that my approach to cybersecurity provides and from the clarity about your business that developing and implementing a good cybersecurity plan provides.

Your business improves because you have resolved issues, and it now runs more smoothly.

Your customers trust you and prefer doing business with you over others beause you protect their data and your product and service delivery is streamlined and they don't experience technical or procedural issues when they do business with you. Revenues increase and you experience greater customer and employee satisfaction and retention.

Doing Good for Others

Your customers know they can trust you to protect their data. They also receive better delivery of service, whether because your operations run more smoothly, or because the technology that they use to communicate with you or order from you is reliable, easy-to-use, and safe.

Your employees' data are protected. Your employees are more satisfied because you resolve issues and avoid or eliminate the problems that would otherwise cause them to be frustrated trying to do their daily work.

If you are focusing more on improving your business because you are distracted, that will result in better service to your customers. You may also choose to provide favorable pricing to your customers because of cost savings from improved processes and workflows. That might result in more sales.

If you produce products for which security is a factor, such as any electronics or devices that connect to the Internet, you build in security. As a result, your products are better for the customer. Communicating what you are doing to make sure your products and services are built with security as a primary consideration makes your offerings more attractive than competitive alternatives.

Doing Good for Your Community and the World.

Let’s start with a disturbing example.

1) Emergency response systems (911) have been taken down by cyberattacks on multiple occasions. Some of these attacks have been made possible because computers owned by numerous individuals have been compromised and then used as weapons against the 911 services. Usually the individual has no idea their computer is compromised, but it is nevertheless being used to take down the 911 system, in league with many other individuals’ computers.

If you do not have good cybersecurity in place, your system may be one of those used in such attacks. The result could be that people die because the ambulance never comes. Nobody was able to get through to 911 because the system was under attack and the calls wouldn’t go through. These attacks have occurred on numerous occasions. And these systems remain vulnerable.

By making sure your systems are protected and do not become compromised, you avoid being part of the attack against critical systems. These systems may be 911 systems, or could be systems that are necessary for Internet communications to work, or water treatment systems that keep your drinking water safe, or the electrical grid.

2) Hackers can use your computer to compromise other people. You may think you have nothing of value. But you know people. And you know people who know people. Maybe you know someone who has an important role in business, in government, in a charity, or other organization. The attacker wants to compromise that company because they are connected to another company that they desperately want to compromise.

They attack your computer and gain information about you. Why you? Because you are friends on Facebook with someone in the company that is the stepping stone to their final target. Or, if you don't use Facebook, they have other ways of finding out whom you know or do business with. So they use information gathered from your computer to impersonate you. Then, they trick your friend into thinking their communications are coming from you and are able to compromise your friend's computer. Now, they have access to your friend and their resources and are only one step away from their final target.

Does this sound far-fetched? It happens all too frequently.

An alternative is that your computer may be compromised simply because it is easy to get into. Then it may be used by the attacker to send out e-mails to a couple individuals at the target company. When those e-mails are opened, that company is compromised.

Keeping your computer safe keeps you from being used as a pawn in the attacker's malicious activities.

3) We have just mentioned a couple ways your computer can be used in an attack against others. There are numerous other scenarios where your computer may be used by a hacker to either facilitate the compromise of other systems or to deliver an attack against other systems. Some of these include stealing personal and financial information from others, distribution of malware, sending out spam e-mail, and extortion. In most cases, people don't realize their computers are compromised and are participating in these attacks.

The Bottom Line

By ensuring you understand and implement good cybersecurity practices, you can become a good citizen in the Internet community. By keeping your computer from becoming a tool of hackers, criminals, and other people with malicious agendas, you can contribute to a safer and better Internet community.

Cybersecurity Is Good For Your Money: Cybersecurity Can Save You Money & Make You Money

Good Cybersecurity Can Save you Money

I've covered most of this already but let's recap.

Doing well with cybersecurity protects your money so that you don't lose it from theft or scams.

Poor security (and failure to put systems in place) results in recurring issues and problems. Implementing good systems and cybersecurity eliminates many of those problems and saves you the cost of fixing those problems as well as the cost of paying employees while they struggle with work slowdowns or outages resulting from those issues.

Smoother operations provides increased efficiency and lower costs.

You avoid having to pay to get your data back because you don't become a victim of ransomware or, if you do, you can easily recover your data yourself without having to pay the ransom.

You avoid the loss of customers due to data breaches and other security incidents. You save the customer and retain their business.

You avoid paying the fines, penalties, or for lawsuits and judgements that could result when you fail to keep customer information protected, when you suffer a data breach, or even just from chargebacks when customers are dissatisfied.

Your systems remain operational rather than being shut down from attacks (e.g., your web site doesn't get hacked, which would result in lost sales until you could get it fixed).

You don't waste money on weak or ineffective solutions but use a strategic approach to get the best return on the money you spend to protect your information and your assets.

Excellent Cybersecurity Can Make You Money

As mentioned earlier, developing a cybersecurity plan can reveal opportunities for increasing your revenue. It may highlight possible new revenue streams that you could easily offer, either directly based on your current operations, or by making small shifts. It may also highlight opportunities where strategic partnerships with other businesses, groups, or individuals can provide signficant additional revenue.

Smoother operations provide better service to customers, resulting in increased customer satisfaction, retention, and more sales.

Cybersecurity Done Well Provides a Strong Strategic/Competitive Advantage

- You gain a strategic advantage over your customers by the reduced costs, improved efficiencies, improved focus, and additional revenue opportunities discovered when implementing a strong cybersecurity program coupled with good implementatin of systems. (All the benefits discussed previously.)

- Additional strategic advantages provided by strong cybersecurity are mainly provided by the communication you have with your customers and in your marketing. You do this by communicating what you are doing in your business to protect information; to reduce issues; to assure the availability of your products and services and your ability to deliver them; and the level of attention you are paying to the interest of your customers in doing all this.

- Part of security is to develop a business continuity plan that will allow your business to survive situations that could disrupt your business. If you do a thorough job with this, you may be in a position to survive events and situations that might otherwise put you out of business. Some of this planning goes beyond the normal scope of business continuity planning but I have developed a framework to do this. This advanced planning framework is especially relevant in light of COVID-19.

  If you do a good job with this kind of planning, you could tell your customers about the measures you are taking so you can continue to provide your services at an expected level. This can reassure your customers that you are being proactive in an effort to continue to support them in light of recent events and hope to be able to do so for the future.

  CAUTION: In light of COVID-19, I would be very wary of how you say this. DON'T make ANY misleading statements or claims. COVID has shown us that disruptions beyond our control can disrupt supply chain and delivery of products to customers, as well as other disruptions. You can develop resilience to address some of this, but to make a claim that you WILL be able to deliver your services despite ANY disruption is misleading and dangerous to your business. Consult an attorney before making any statements that might lead your customer to arrive at unrealistic conclusions. Don't Make Such Statements.

- If you offer products or services for which security is a factor (essentially any electronic or Internet connected device, or a product or service that collects or processes data) you should give serious consideration to the security implications of having and using that product or service. You may need to consult with a security expert to help identify those factors. Then address any concerns or issues in the design of those products and services and make sure they are secure.

  Many products are released which do NOT take into account the security and privacy issues involved. These are not limited to physical products, but can even include web sites where information is collected, or where the customer submits material, including audio, video, comments, etc.

  If you do an excellent job in considering security when developing and releasing such products and services, you can communicate how security has been an important part of the process of designing and delivering your product or service. Many customers do care about security and about privacy. Regulations are being put in place to enforce that. Communicating your efforts can offer you a real competitive advantage.

- When customers have confidence that you are keeping their data safe and looking out for their best interests, they trust you more and are more satisfied This results in greater commitment to your brand. As part of this, they are likely to make the assumption that, if you are taking significant measures to implement good cybersecurity in order to protect them, you care about them and will consider their interest and will go the extra mile to take care of them in other areas as well. Hopefully, that assumption will be backed by your efforts to so.

Final thoughts

By now, I hope that you recognize that ignoring cybersecurity is bad for your business.

Taking a strategic approach to cybersecurity provides health benefits to you due to reduced stress, worry, anxiety, and/or loss of sleep. It also provides numerous benefits to your business.

Security done right is not about following annoying rules that keep you from getting your work done. It is about putting effective practices and systems in place that enable your business to function with reduced risk and with smoother operations. There may be times that good security involves more effort, such as using a password or other mechanism to access sensitive data. But a reasonable approach will minimize the impact upon your operations caused by this increased effort and will strive to find a way to protect your information and systems effectively, in as nonintrusive a manner as possible. It will simultaneously provide significant roadblocks for those trying to behave in a manner that threatens your business and data.

Security can provide cost savings through reduced costs and increased efficiency. It may be that the design and implementation of good security may result in an increased expenditure but, done right, cost vs. benefit is an critical factor considered during the selection of security solutions. A well-done security implentation doesn't spend too much on security but delivers sufficient benefit to make it well worthwhile. The best choices will allow at least partial recovery of costs through the savings obtained by reduced spending on fixing problems and increased efficiencies.

Good cybersecurity can also make you money. This doesn't happen by accident. But an excellent plan will include this element and provide the information, insights, and opportunities to increase your revenue. This alone could be enough to more than pay for the entire cybersecurity program. Implementing such a program could turn cybersecurity into a profit center.

A lot has been said about putting "a good cybersecurity program" in place. The benefits do not occur by default. Simply following common sense and implementing oft-repeated recommendations is not enough. To receive the benefits I have outlined, one needs to understand cybersecurity, the business in question, the threats and the vulnerabilities, and the measures one can put in place for protection.

In addition, to achieve the greatest benefits, one needs a certain orientation, which includes risk management and governance, as well as creative thinking and an understanding of ways to turn security planning into a competitive advantage. It also relies on the ability to identify new sources of revenue and strategic partnerships.

What’s next

I highly recommend you learn more about cybersecurity. It doesn’t have to be hard. While there are areas of cybersecurity that are highly-technical, even the non-technical business owner can acquire a very good understanding of cybersecurity if given the right resources and guidance. One can always call a technical expert for the technical areas. But you can achieve a good understanding of cybersecurity from a high level without the need to get technical. That kind of understanding is something that the majority of technical experts don’t have, unless they happen to be certified cybersecurity experts.

When you requested this e-book, you also subscribed to my e-mail list. Watch for more information by e-mail. Those e-mails will be easy-to-understand, bite-sized chunks.

As time goes on, I expect I will offer classes or workshops, which will go into more depth and will actually allow you to implement the understanding better than the small chunks in the upcoming e-mails.

If you want to explore how your business can do a better job with cybersecurity, you may contact me.

I can be reached at: phil@smallbizcybersec.com
You can find my web site at: http://smallbizcybersec.com/