Collection

Users can Collect posts into a printable, sortable format. Collections are a good way to organize posts for quick reading. A Collection must be created to tag posts. More Help

Thread:	Ron Pionk CySe Impact on Small Business	**Posted Date:**	September 29, 2019 9:54 PM
		Status:	Published
Post:	RE: Ron Pionk CySe Impact on Small Business	**Overall Rating:**	
Author:	**LEAH DREW**		

I agree that putting a smaller plan in place at the start is a good idea. I also think it's important to take into account the changes in industry, and not just to build on the original plan if it's become outdated. They should conduct a risk assessment every year when planning their yearly system and budget, which might mean that they spend either more or less than they had the previous year, depending on what's most important and how much money they're willing to spend. I think a plan that is revised every year can protect a business much better than a yearly plan that doesn't innovate. Even if they haven't expanded their budget at all, they still need to be able to adapt.

(Post is Read)

Thread:	Small Steps for Small Business Security	**Posted Date:**	September 29, 2019 9:21 PM
		Status:	Published
Post:	Small Steps for Small Business Security	**Overall Rating:**	
Author:	**LEAH DREW**		

Small businesses are a major target for cybersecurity events because their defenses are usually easier to penetrate, so it’s important that these businesses develop a cybersecurity plan. The first step should be to conduct a risk assessment in order to understand what needs to be protected, as discussed in our reading. This is an important step because every business is different, and some businesses and industries have unique threats and vulnerabilities that need to be taken into account. Money should be focused on where these threats and vulnerabilities lie. When determining where to spend money, a small business should have some plan in place to address each of the core functions of the Cybersecurity Framework: Identify, Protect, Detect, Respond, and Recover.

However, there are always less costly steps that small businesses can take to protect themselves, and it’s important that businesses research every so often to find out what threats are affecting their industry. As an example, an article published by entrepreneur.com titled “3 Biggest Cybersecurity Threats Facing Small Businesses Right Now” states that some of the most pressing issues for small businesses are Internet of Things leaks, opaque algorithms, and legal action against security researchers. The Internet of Things is a network of common devices such as alarm systems, GPS, and medical equipment, which can be easily taken advantage of because businesses don’t always secure them. An easy step that all small businesses could take is to make sure to change the default passwords on these devices so that they’re harder to hack into. Many organizations depend too heavily on algorithms, which can be faulty and even leave security holes if they aren't monitored. Critical decisions should be made by a human, and algorithms should be monitored or even eliminated if possible. Finally, there is an increasing trend of security researchers being silenced by manufacturers. This means that there are fewer whistleblowers able to inform small businesses about security issues with the technology that they purchase. Small businesses should insist on transparency and be cautious when buying from a producer that isn't transparent with their consumers.

Overall, when a small business develops a cybersecurity plan, the benefits should outweigh the costs. The business should maintain security by regularly researching which threats are affecting their industry, because the examples listed above will change, and not all are applicable to every business. A cybersecurity plan should be centered around the threats that would have the most impact on the small business.

(Post is Read)

← **OK**