Introduction

If you haven't been hit by a virus, malware, ransomware, or a breach, you likely know someone that has. The damage, cost and bad publicity of these incidents are obviously best avoided if possible. Knowing that security incidents can be devastating is one thing, preventing them is another. If your cybersecurity experience is limited, or if you are without technical resources, even knowing where to start can be a problem. There are a couple of options at your disposal that can get you off and running and will cost you nothing.

The first option is a call to the IN-ISAC (317-234-3434). The IN-ISAC is a part of the Executive Branch of state government. One of its duties is to help those local governments, K-12, higher-education, and small businesses in need of cybersecurity help. We have a CISSP and former CISO on staff looking for ways to help those in need.

The second source of help lies in the remainder of this document. We've developed a brief playbook that can get your cybersecurity effort started quickly. If you have done any investigation into the subject you already know cybersecurity can be shrouded in acronyms and technical complexity. You also know that the sheer volume of information can be overwhelming. Both of these factors drove the development of this document. It is concise and we remove the jargon where we can. In 10 pages you will have the information needed to formulate you plan. It's not all that will you need for a complete program but it does get you started with those things that are most important.

Getting Started

Protecting your data related assets is work. The good news is that success depends much more on discipline than technology. If you understand risk, make good business decisions, and establish controlled processes, you will achieve your goals.

Playbook Outline

This document has three objectives.

1. Provide direction to organizations needing to begin or expedite an effective cybersecurity program
2. Prioritize the actions that are most likely to stop a breach
3. Ensure the actions prescribed in this guide fit into the longer term goal of a more comprehensive program

If you have done any research you've likely come across a few security "frameworks". These frameworks are essentially playbooks you can use to build your cybersecurity program. In order to cover every aspect of cyber security they become quite voluminous. Everything you find in our document can be found in those frameworks. We've just cut to the chase based on our experience.

A quick note on the frameworks. Most would say that if you are going to adopt a framework, make it the NIST framework. We agree with that wisdom. The NIST framework is comprehensive and well supported.

The Playbook Overview - Recommended Steps

Below is an outline of the steps to consider to eliminate risk as quickly as is possible.

1. Put someone in charge
2. Identify the bad things you don't want to happen (risk assessment)
3. Steps to mitigate risks
    a. Address the human (ATH)
        i. ATH1 - Acceptable use agreement policy
        ii. ATH2 - Cybersecurity training
        iii. ATH3 - Comprehensive body of policy
    b. Safety net protections (SNP)
        i. SNP1 - Firewall
        ii. SNP2 - Tape backups
        iii. SNP3 - End point
        iv. SNP4 - Two-factor
        v. SNP5 - Email filter
        vi. SNP6 - Network monitoring
        vii. SNP7 - Internet filter
        viii. SNP8 - Independent pen test
        ix. SNP8 - Encryption
    c. Hygiene (H)
        i. H1 - Patch
        ii. H2 - Harden
        iii. H3 - Segment/isolate
        iv. H4 - Least privilege
        v. H5 - Password complexity
4. Be ready when disaster strikes

A Concise Expansion on the Steps

Step 1 *– Put someone in charge*
Depending on the size and complexity of your organization and your risk profile, this may be a full time position or a part time position. There is work to be done that requires responsibility, accountability, and empowerment. More important than being a security expert, the person selected should be trusted with demonstrated common sense and a proven work ethic. There is a learning curve but if they're willing to work and learn they will be able to succeed.

Step 2 *– What would be harmful?*
What are the cyber things you don't want to have happen? In security lingo, this is a risk assessment. You can do a web search and find a number of different formats for risk assessments. The problem is, at 50 pages or more of acronyms and jargon, those documents might defeat you before you get started. For our purposes we're going to keep it simple. Answer these questions:

- What do we have that we have to protect? Assets
- What can go wrong with our important assets? Threats
- What are the ramifications if the bad things happen? Damage

Put your answers into a spreadsheet that can be as detailed as you want or as simple as the example below.

Assets	Threats	Damage
Cash/Funds	Loss or Theft	Damage to constituents, loss of public trust, loss of integrity
Confidential information	Unauthorized access (loss or leakage)	Damage to constituents, loss of public trust, loss of integrity
Online utilities	Unauthorized access, natural disasters	Public safety jeopardized
Physical assets	Loss or theft, natural disasters	Service disruption, budget impact
Service delivery capabilities	Ransomware, DDOS, natural disasters	Service disruption, budget impact

To round out this exercise requires a little more work. You want to create an asset list to understand all that you have and to make sure nothing is overlooked. Hardware devices are the first things that will come to your mind. You also need to think about your systems and your data. It might not be instinctive to think of these as assets until you realize how your business would suffer without them.

Data can be especially elusive asset to protect. A quick example shows why. Let's say hypothetically that you have a list of 1000 customers. You have their name, date of birth, SSN, address, and phone number in a database stored on an internal server. You know you have to protect that database and you do a pretty good job of it. It starts to get a little messier when you count the copies of the database, or parts of the database, floating around elsewhere that may only have minimal protections. It's possible some of your staff have a copies of the database in spreadsheets stored on their laptops. You also know you back it up to the cloud. It was copied to a couple of flash drives as well. Now you're left with several copies of the same data and maybe only one is appropriately protected. The multiple copies of this one asset raises the quantity of risk that something goes wrong. In this case you need to protect each instance.

Scenarios as the one above are common and frequently necessary for business success. The key is to manage each copy, determine if all are needed, eliminate those that are not, and protect those that are.

With your list of assets in hand, the next task is to prioritize your risks. This step can be challenging at first but you will soon get in the swing of things. Identify the damage that could be done and how likely is it to happen? Rank the damaging events in the priority that concerns you most. You then take actions that reduce the likelihood of these events becoming reality. Assets of high value with a high likelihood of being lost, stolen or damaged, accompanied by dire consequences should they happen, become your high priorities. If the asset is of lesser value, has a lesser likelihood of loss, and the damage is minimal if it happens will be a lower priority. This determination is going to be subjective based on the nature of your business. Prioritizing risks allows you to address those urgent issues first which drives down the likelihood of something catastrophic happening to your organization. Fortunately, you can address more than one risk at a time.

Step 3 *– Getting down to business*

Above we took the necessary steps of identifying your assets. Now we're going to identify the scenarios that are likely of most concern, those that can do the most damage. Remember, this focus is on cybersecurity. At times there is an overlap with physical security and possibly even public safety. If that is the case the overlap needs to be considered and prioritized accordingly. Because those scenarios are not common for most organizations, the three scenarios of most concern are:

- Loss of funds – Someone hacks into your system and gains access to systems allowing them to move your funds without authorization. Or, they trick your staff into doing it for them.
- Catastrophic loss of data – A fire or tornado or other event damaging your facilities and destroying your data as well. Ransomware can have the same result.
- Security breach – The loss of your data to hackers via social engineering, primarily through phishing emails, is the most likely of the scenarios you have identified. Social engineering is said to be the starting point for 95% of all breaches and phishing is present in 90% of those cases. To be clear, you can run into other trouble.

There are other aspects of cybersecurity that you need to address. We are jumping to those of highest importance. Your environment may already have some of these measures in place. If so, confirm they are doing the job as expected. If not, a new direction may be needed. Finally, the steps below are not intended to be linear or in order of priority. Identify those that eat up the most risk the fastest. Fortunately, you can work on many of these measures in parallel.

Address the Human (ATH)

Even those unfamiliar with cybersecurity have heard that humans are the weakest link. This is because they are involved in every aspect of your business in one way or another. You need your people but they make mistakes, sometimes without knowing it. Here are some things you can do that will quickly help your workers do the things they need to do and cut down on their mistakes.

Suggested controls

ATH1. An acceptable use agreement – provide guidance to the users of what they can and cannot do with your assets. Here are key points to consider:

- Find a template that you like through a search. There are thousands available and it will save you from recreating the wheel.
- Insert legal and HR resources in the process of finalizing the agreement.
- Ensure it is enforceable by writing realistic expectations.
- Enforce it fairly and uniformly. Don't paint yourself into a corner with language that is too rigid.
- Keep it brief – Cover the important guidelines concisely. A document that is too long with onerous requirements will work against your intentions.
- Make them sign it – Whether electronically or in ink, make sure they understand there is accountability for adhering to the terms.

Comment: Most workers will adhere to guidance provided by your organization and that cuts down on risky behaviors. Templates for acceptable use agreements are readily available and modifications to your needs should not be difficult. It can be more difficult getting the document distributed, agreed to, socialized, and preferably training upon, might be a little complex. This has a high return with the costs being researching and modifying the template.

ATH2. Cybersecurity training – Give workers some exposure to cybersecurity fundamentals and it will pay dividends. Train them on high risk issues such as phishing, social engineering, data classifications, and malware first. There are other training topics that can wait for later. Comment: Phishing is a great place to start as that is where the majority of breaches begin. Training will cut down on clicking on malicious email links and opening malicious attachments. Comment: To let you know how important this can be know this. If your employees are never fooled by a phishing message you will probably never have a breach. Training is fairly easy to find with a web search. There are no cost options, low cost options and some that are expensive. Worker interest and absorption are hard to obtain. Mandated training is often resisted and is often boring. Cybersecurity is not going to be any different. In your research seek programs that are interesting and interactive. To drive home the point, make sure workers know that the training is mandatory and important, and that there is accountability linked to HR for failures.

ATH3. Comprehensive policy – The acceptable use agreement is an example of a policy. Others are needed and a framework should be adopted. Crafting a full body of policy can be time consuming though templates are again available. The recommendation is to start with the acceptable use agreement and others that cover topics such as email, data handling, and passwords, first. Then circle around and get the remaining needs until complete.
Comment: For the long run you need a comprehensive body of policy. However, this can take a while to develop. Cherry picking important policies to develop as you look to mitigate risk quickly is recommended. Over the long run policy development is not hard given all the templates available. It does take some time to maintain. Neither of those two points make it "hard." The hard part is socializing your policy in a manner that makes it a living and breathing document for your workers rather than a dust collector. One key point of guidance. Never write a policy that you don't intend to enforce.

Safety Net Protections (SNP)

Safety net protections may be the place you want to start in order to protect your assets. Dealing with the human factor is difficult and has one unavoidable certainty. No matter what you do people will fail. In truth, so will the safety net protections we are going to discuss below. But these protections may be more reliable and mitigate more risk making them the ideal place to start. You will execute many of these measures in a parallel rather than a linear fashion.

Suggested Controls

SNP1. Firewalls – A fundamental protection protecting the internal network from the outside. It almost goes without saying this is a critical defense and primary requirement for security.
Comment: You may read that networks no longer have perimeters but having a firewall in place protecting your network is indispensable. A base setup for a firewall is not difficult but is also not a place where you want to have a mistake. The more complex your network, the more demanding it becomes.

SNP2. Backups – Most people know they need backups. The problem is having the discipline to make sure they are done on an appropriate schedule, that the backed up data is adequately separated and protected from the risks on the production network, and that the restore process works. Natural disasters and ransomware can decimate businesses. Backups can save them.
Comment: There is no step more important to the survival of your business than a solid data backup plan. It can rescue you when there is fire or weather damage to your facility. It can do the same if you get hit by ransomware. There are a number of technologies and options available and they are easy to setup and maintain. You do need to test the recoverability of your data through exercises which might be a little more complex. There are many options available. Pick the one that works best for your organization.

SNP3. End point – In the past, this product was referred to as anti-virus but it has morphed into a tool providing more advanced and capable protections. This key protection serves as a front line defense for human error for devices on and off the network. To sum, it is indispensable. If you are still using a signature based product you need to upgrade.
Comment: This is the premier safety net for human error. It won't stop everything but a good product will stop a high percentage of potential end point infections. The products are getting easier to support. In the past they could be very labor intensive which drove the total costs of this type of protection up significantly. There are options ranging from free to expensive. If you've got some budget this is a place to carve some out for a good product. You won't regret it.

SNP4. Two-factor – The technology options are numerous and are becoming more affordable all the time. This layer provides protection when someone in your organization has had their credentials compromised. It can stop someone that has your IDs and passwords from accessing your network from their couch in Russia. Properly configured this technology will stop a number of common hacking attacks. It does add some inconvenience at login but it is worth it

and the adjustment period is very short. Solutions have become easier to implement and easier to use. Support difficulty will depend on the solution selected. The cost for two factor has decreased as its use and competition have grown.

SNP5. Email filter – This technology may already be incorporated for those with cloud based email. For those with an in-house email system a filter can cut down immensely on the amount of non-legitimate email messages. It may also recognize phishing scams and stop them before they get to end users.
Comment: It is hard to imagine any business with any sort of email system not deploying filtering. It cuts out at least half of the messages (spam) targeting you organization. It will add complexity to your email system. You will need staff to support it for an in-house solution and the filter will make mistakes (e.g. – let things in it shouldn't, block things it shouldn't). There are multiple options available including cloud based solutions. Costs are coming down as a result.

SNP6. Network monitoring – This can be extremely complex and labor intensive to build in house depending on the environment. It is a valuable layer and there are many outsourced services that can provide a valuable set of additional eyes to monitor your network traffic.
Comment: This is a tool where the value is not necessarily based on the number of events it identifies. You just want to have confidence that it will identify those that are potentially destructive. It can take time and expertise to tune the system and ferret out false positives. Outsourced services have some advantages to consider. Historically this has been an expensive labor of protection whether provided in-house or externally but prices have been falling.

SNP7. Internet filter – This tool allows you to set parameters around what type of web surfing workers can do. It can identify malicious web pages and block users from accessing the site, it can stop workers from accessing inappropriate and/or controversial sites, and has other limiting capabilities that may be of interest.
Comment: The value of this device depends on your organization's culture. If you lock it down to work related Internet use then your risk of malware infections goes way down. Users cannot visit nefarious sites and links in phishing messages will be blocked as well. It can take some labor to configure and maintain as the websites needed for effective business grows. If your organization is not going to restrict web surfing this will be of much less value. The cloud has brought additional options to the standard in-house appliance approach that dominated the market for some time.

SNP8. Independent pen test – A pen test was placed here though it could be argued it is better suited for the hygiene category. Regardless of where we place this recommendation in the document it is a very important option to consider. An outside party will find problems with your practices and defenses. The problems identified will help in the establishment of priorities. The pen test findings can set your security priorities as you look to shore up your defenses.
Comment: It is not always fun but it is always good to get a check-up. Even if you have solid defenses they will find something to show their value. If you leverage competition you will likely find this service to be within most budgets. Especially, if you allow the work to be done remotely.

SNP9. Encryption – Encryption will protect your data if it is lost in many circumstances. This is particularly important with laptops
Comment: There are many aspects of encryption. It is important to understand where encryption will give you expected protections and where it will not.

Hygiene

Most computer breaches take advantages of weaknesses in software that have been known about for months and years. If your business can implement fundamental, disciplined processes, you will be far ahead of the game.

Organizations that maintain hardened, current systems are much less susceptible to cybersecurity problems than those that are not.

H1. Patching – Security patches are very important to minimize the risk of a malware infection. All software on servers and workstations should be monitored and patched in a timely manner. Servers are typically a little easier to regulate than workstations. At the workstation, if you can patch the OS, Adobe, and Java on a monthly basis you will be at much less risk for a malware infection. Don't stop there but make sure that is where you start.

H2. System hardening - This effort, and it can be an effort, eliminates unused software and services. This is usually harder to accomplish from a cultural perspective than a technical standpoint. The more software that is needed on a device the more difficult it will be to harden from a technical standpoint.

H3. Least privilege – This key principle of security states that workers should only have access to the information and tools needed to do their job and no more. This is frequently not the case. It can be difficult to take back access once it has been given. Be sure to separate the duties of your admin team. They should have one ID to do their administrative work and another ID for their non-admin work (e.g. - email, web surfing, etc.).

H4. Isolation/segmentation – Network segmentation can be an effective means of limiting access to your important data. Conceptually, many of your workers may have access to non-confidential data but the data that needs protection can only be accessed by only those that need it to execute their duties.

H5. Password fundamentals – Ensure your passwords are secure. One trend with password protection that makes things a little easier is the acceptance of a long password versus a shorter one with complexity. A longer password can eliminate the need for special characters. A 24 character password, what is frequently called a passphrase, will be more secure than a 12 character password requiring a capital letter, special character and a number. As important as anything in the password realm is to ensure they use their work password only at work. More hackers are building profiles on individuals and attempting to access work systems with a password compromised elsewhere.

Incident response

The things we have discussed above give you a good plan of attack for your security program. Our preference has always been to prioritizing the prevention of a problem rather than on the response to one. However, it is only prudent to be prepared should something go wrong because something will go wrong. Knowing how you will respond, either with your staff and/or external resources, can be key to quickly identify problem and possibly limit the damage.

1. Outside resources – Know you're hired guns. Have at your ready a list of those that might be able to help in an emergency. This can be local technical resources, outsourced or cloud provider, the Indiana State Police, your local law enforcement, your insurance agents, and the IN-ISAC. Understand the readiness of each resource to assist you as you deal with the incident.
2. Run through an exercise – Pick out an event from one of the many scenarios you read about in this document and talk with your team about what you would do if you were in their shoes. In just a few minutes you can figure out the things you need to have (e.g. – cell phone #'s, key contacts, after hour's procedures, etc.). Think through your contingency plan. Have an idea of where you would relocate and how you would handle down time.

Conclusion

Cybersecurity can seem like a mountain too tall to climb. However, with the ropes and ladders we've provided here you can conquer the challenge. The hardest part is simply getting started. Once you get into it you will find you can succeed. Use the information in this document to focus on those items most important. There are many other important and useful controls that you will need to incorporate as your program matures but this should get you started.

If you have a question, related to this plan or any cybersecurity matter, we are glad to talk through the issue with you (IN-ISAC - 317-234-3434).

Phishing Layers of Protection and the Role of Each

Let's take you through common attack scenarios, primarily around social engineering/phishing where it is said more than 90% of all breaches originate, to show the layers of protection our approach builds in.

Layers

Layer 1 - Worker makes us proud. They keep their computer activities strictly business as outlined the acceptable use agreement (ATH1) for guiding our workforce to safety. They don't surf non-business websites, they don't use unauthorized flash drives, they are angelic and our organization never has to worry about a breach.

Layer 2 - Worker makes a mistake and gives hackers their ID and password in a phishing scheme. Fortunately, when the hackers try to use those credentials from Russia, even with the correct ID and password, they can't get in because we require two-factor authentication layer for remote access. (SN

Layer 3 - Inbound phishing message, and a darned good one at that, is heading our way. This message is really believable, we're going to see infections, lose credentials, and maybe even have to fight ransomware. Fortunately for us, we have an email filter that recognizes the email as phishing and it never arrives at the desktops of our workers. (SN

Layer 4 - Uh-oh, this time we're not so lucky. The well-crafted phishing scheme has evaded our email filter. However, we are overcome with pride and start looking for capes in the office because our workers/super heroes recognized the phishing message and deleted it without opening it. We see the dividends from investing in user training. ATH

Layer 5 - Oh no, phishing message slips by filter and tricks workers. We are doomed. But wait, our end point protection springs from the workstation and stops the malware before it can do its damage. Another bullet dodged! SNP

Layer 6 - This is bad. Phishing message evades the email filter and tricks our user into opening an attachment or clicking on a link. The malware uses an innovative method to activate that our endpoint doesn't recognize. The malware starts to activate by reaching out to the Internet for additional instructions and to download nefarious components. Fortunately, we escape harm because we have our Internet filter on and tightened down to allow only trusted sites by a whitelist. Thanks to the Internet filter and our foresight to limit web access we remain safe. SN

Layer 7 - It's been one of those days. Everything's gone wrong and now a phishing message evades the filter, tricks our user, isn't recognized by our endpoint protection, and doesn't use the Internet to activate. Time to update the resume. This malware can exploit weaknesses in the Microsoft OS, Java, Adobe Reader and Adobe Flash. Yet we are again saved. The malware cannot activate because our crack technical staff have made sure that our laptops, workstations and servers are all updated with the latest security patches as soon as they come out. H & H

Layer 8 - You see how this is going. Now the phishing message evades the filter, tricks the users, gets by endpoint protection, doesn't use the Internet to activate, and even though we're patched, the malware is able to activate. Man that is disappointing after all the cash, time and effort we've spent on the layers of protection that failed in this case. We're breached. Fortunately, all is not lost. In fact, nothing is really lost. The infected user only had access to non-confidential data. Better yet, our network monitoring picked up on the malware activating. We get the word on the problem and we reimage the device before any damage can be done. H & SNP

Finally, the worst case - Let's take a little different tact. A phishing message came our way but we hadn't trained our people. They didn't know any better and since we don't own a filter, they also surf any site they want on their lunch hour. The free end point protection package we downloaded doesn't catch the malware when our worker clicks on the link in the phishing message. Since we haven't done any of the fundamental things above, there is no reason to pretend

we're patching our devices and honestly we didn't even know network monitoring was a thing. The employee that clicked on the link is also our server admin and we don't restrict their account in any way. Boom! All of a sudden we can't access our data and a dialogue box on the screen tell us that we owe a Bitcoin ransom. We simply can't afford to pay what they're asking and we're not sure our data would come back even if we did. As incompetent as we are, we do 1 thing right. We take a nightly backup of all our servers and store that back up in our vault. Now it still hurts and it's pretty embarrassing to talk to the media about our failures. But over the course of a couple of weeks we get our servers back up and we're making progress on getting all of our workstations reimaged. After a month, though, we're fired. They said we were responsible and the media scrutiny just won't allow them to continue without hanging the incident on someone. Our replacement comes in and starts implementing the protections we failed to put in place. It's easier for them because people have seen the damage a breach can do. It is a powerful motivator. At our new email address, where we're now employed as a greeter, we get an email from the new person that says, *"This place was a breach waiting to happen. If you don't believe me just come on by and I'll show you the results from the pen test we just completed. Even in digital format you can almost smell how bad it stinks. Thank you for creating an opportunity for me where such a long honeymoon is guaranteed. Oh, and thank you for at least doing the backups. We can rebuild everything else over time but without the data they might have just decided to shut us down! Thanks again. New Person"* This email haunts our mind as we welcome the next person to our store.