INFO ADVANTAGE

How To Build A Cybersecurity Program 90 Days Or Less

A Practical Guide for Busy Executives That Want to Address Their Cybersecurity Concerns Now!

The industry reports and associated statistics are all providing the same fundamental insight about the state of cybercrime. A quick internet search of "Cybersecurity Trends" will consistently deliver similar basic findings. A survey of the people you trust in your professional network about cybercrime concerns will yield common, if not identical, feedback.

There are two simple truths related to cybersecurity.

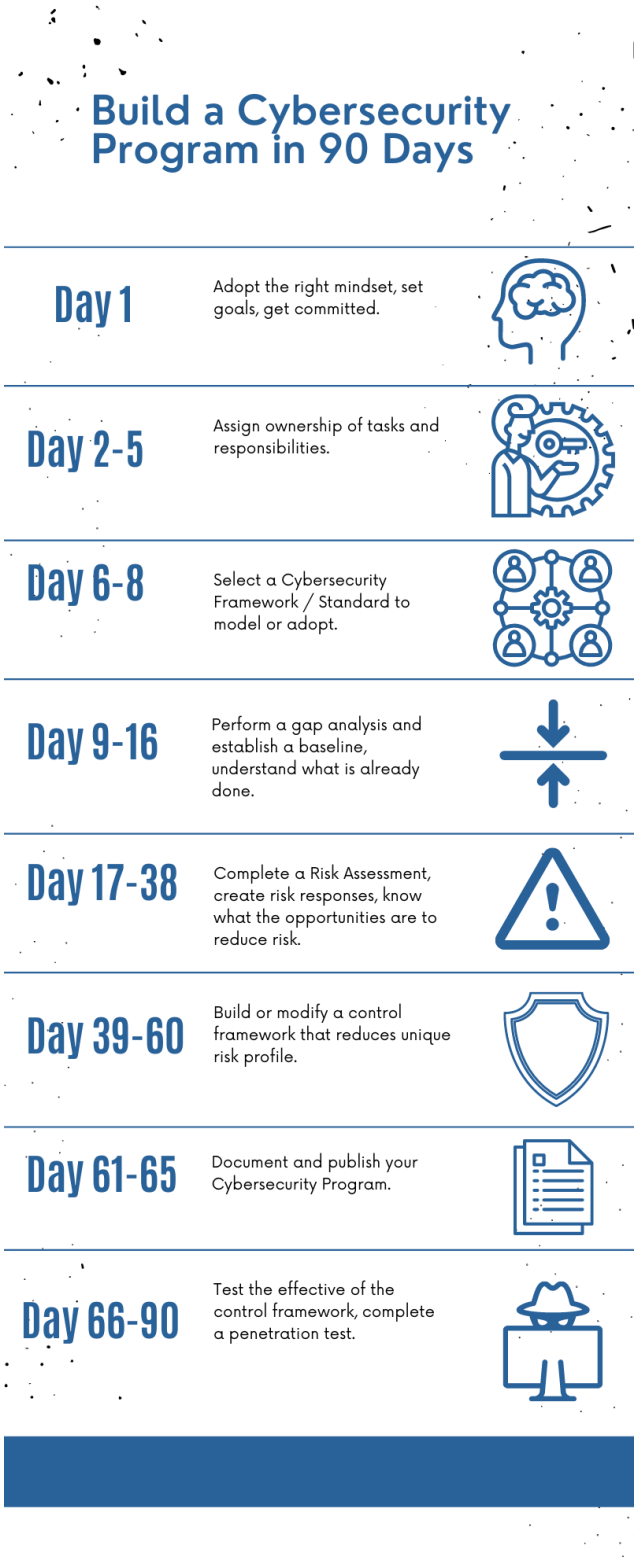
1. The risk and exposure related to cyber threats is at an all-time high and it is only getting worse.

2. Most organizations are struggling to build and maintain effective cybersecurity programs.

Executives must realize by now that there is a thriving, in fact – BOOMING cybercrime economy. They must also realize by now that the organization they work for is a prime target of malicious hackers. Furthermore, executive must also recognize that successful cybersecurity attacks can have great consequences like lost careers, financial ruin, squandered opportunities and even threaten business solvency. Yet for some reason, most executives have failed to accept the responsibility bestowed upon them to develop effective cybersecurity programs and reduce overall risk. Perhaps the "failure" is not necessarily accepting that responsibility but instead the "failure" is taking proper action.

This whitepaper is designed to help executives develop an effective cybersecurity program in 90 days or less. There are eight high level tasks that must be completed over roughly 90 days. Each task will be discussed with the intent of providing a high-level understanding of the work that needs to be completed. In addition, links to resources that may help with the execution of each task will be provided as well as a list of typical roles, skillsets required to complete the task.

The picture below provides a visual representation of the eight high-level tasks with the associated timeline for completion.



Day 1 – Adopt The Right Mindset

If we wish to accomplish most tasks, we have to remove any unfavorable biases about that task from our minds. Addressing cybersecurity concerns can be hard, annoying, unattractive, or downright overwhelming. But you must appreciate the fact that it needs to get done. So do a few things to get your mindset right:

1. Set a goal – write down the following statement "I will create a cybersecurity program this month". I didn't say "I might" or "I can try to" I said, "I will". I will statements are powerful. It is an expression of commitment!

2. Write down the benefits of completing the task. What good will come as a result of you creating a cybersecurity program? Perhaps the sense of safety and security, perhaps the confidence that you can survive a cyber-attack, maybe it is a resume builder, or perhaps it can be leveraged in sales and marketing strategies. Maybe you can rest assured that the next audit will go well. The benefits have to be meaningful to you but write them down. It will give your effort purpose.

3. Lastly – write down the perceived roadblocks or challenges and what you can do to either avoid them or respond to them as you accomplish the task of creating a cybersecurity program. Perhaps you will have to learn more about the topic. Maybe you are worried about the resources it will take to accomplish. If you think something will get in the way of progress – write it down – then write down some tactical ways to handle those problems. This way when you are presented with a roadblock – you will already know how to handle it.

Helpful resources: *Goal Setting Worksheet – Found in Appendix A*

Required people / roles: *CEO, Information Technology Leadership*

Day 2-5 – Establish Ownership

The second step in creating an effective cybersecurity program is to clearly assign ownership of tasks and responsibilities to yourself or others. This will not get done if someone is not responsible and held accountable for specific tasks and deliverables.

Depending on the anatomy of your organization, ownership of building the cybersecurity program could be centralized and delegated to single person or it may be distributed amongst several people or groups of people. Treat this mission like you would any other business objective. Select the right people to execute, assign them formal responsibility and be prepared to hold them accountable for results.

Helpful resources: *https://niccs.cisa.gov/about-niccs/workforce-framework-cybersecurity-nice-framework-work-roles (note, many of these roles will not be needed in smaller organiations, but delegation of responsibilities should still occur).*

Required people / roles: *CEO, Executive Leadership Team, Human Resources*

Day 6-8 – Select A Cybersecurity Framework To Adopt

The good news about building a cybersecurity program is that there are a number of standards-based frameworks available to adopt. These frameworks provide the prescriptive guidance you will need to build impressive cybersecurity defenses and reduce your overall risk. You do not have to re-create the wheel. The frameworks are created by standards organizations and adopted globally. Think of it as selecting a recipe to follow.

Examples of Cybersecurity Frameworks to consider are:

1. NIST Cybersecurity Framework
2. ISO / IEC 27000 family
3. Center For Internet Security (CIS) 18 Critical Security Controls
4. Control Objectives for Information and Related Technologies (COBIT)
5. Cybersecurity Maturity Model Certification (CMMC)

We highly recommend adopting the NIST Cybersecurity framework. NIST stands for National Institute of Standards and Technology. The framework consists of five concurrent and continuous Functions which are Identify – Protect – Detect – Respond and Recover. Each function has underlying categories and subcategories of content. Essentially this framework encourages organizations to be capable of (1) Identifying threats and risk , (2) Protecting themselves against threats with appropriate security controls, (3) Having the ability to Detect anomalies, and potential cyber-attacks, (4) Being able to Respond to those attacks in a methodical way and lastly (5) Knowing that there are Recovery strategies in place to restore normal business functions.

Helpful resources:

1. NIST CSF - https://www.nist.gov/cyberframework
2. ISO / IEC 27000 family - https://www.iso.org/isoiec-27001-information-security.html
3. CIS 18 Critical Security Controls - https://www.cisecurity.org/controls/
4. COBIT - https://www.isaca.org/resources/cobit
5. CMMC - https://www.acq.osd.mil/cmmc/draft.html

Required people / roles: *CEO, Information Technology Leadership*

Day 9-16 – Establish A Baseline

At this point we now have a prescriptive standards-based framework that we can use to guide the development of our cybersecurity program . But we want to be careful about duplicating previous efforts or doing work that has already been completed.

Most organizations already have fragments of a cybersecurity program implemented. For example – The NIST Cybersecurity Framework says that you need to have a Disaster recovery plan in place. If you already have a suitable DR plan – then you obviously do not need to write a new one! NIST also says that you must test your DR plan. Perhaps you are not doing that today.

So when we say that you have to establish a baseline – the objective is to complete a gap assessment. Compare the current state of your cybersecurity program – even if it is sparse and fragmented – to the NIST cybersecurity framework (or alternative framework selected). Understand your "Current State" and develop an action plan based on the Gaps that exist to achieve your desired state. Many times, you will need the help of cybersecurity experts to help you complete a NIST cybersecurity maturity assessment. It is critical to establish a baseline and understand what needs to get done to achieve compliance with the standard.

Helpful resources:

1. NIST CSF - https://www.nist.gov/cyberframework
2. ISO / IEC 27000 family - https://www.iso.org/isoiec-27001-information-security.html
3. CIS 18 Critical Security Controls - https://www.cisecurity.org/controls/
4. COBIT - https://www.isaca.org/resources/cobit
5. CMMC - https://www.acq.osd.mil/cmmc/draft.html

Required people / roles: *CEO, Information Technology Leadership*

Day 17-38 – Complete A Risk Assessment

Step five is perhaps the most important step in the entire process. When someone asks, "should I implement a multi-factor authentication solution or network segmentation? I only have enough resources to do one.." I tell them to **implement the one that will reduce the greatest amount of risk.**

How do you know what cybersecurity controls will reduce the greatest amount of risk? Well – you have to know where your risk lies. A risk assessment is an exercise that will define your unique risk profile and allow you to build an effective cybersecurity program that is strategically designed to reduce risk. That is why a risk assessment is a foundational element found in any cybersecurity program,. Remember, we have limited resources, so we must use them wisely.

There are three primary steps taken to complete a risk assessment. First, your identify all the bad things that can happen. We call these bad things "risk events" and typically place them in one of four categories – Accidental Risks, Adversarial Risks, Technical Risks, and Environmental Risks.

Then for each risk event we ask ourselves "how likely is it that this will occur?" and then "what will the impact be if it does occur". Answering these two questions allows us to calculate a risk rating for each risk event. If a risk event has a high likelihood of occurring and will have a very high impact on business operations– then the risk rating will be high. Alternatively – if a risk event has a low likelihood of occurring and will not have a material impact on business operations then the risk rating will be low.

Once you have assigned risk ratings to all risk events you will have a naturally prioritized list of opportunities to improve your cybersecurity controls. There is no such thing as being 100% secure. Our goal is to allocate precious and limited resources in a way that provides the greatest opportunity to reduce risk.

Helpful resources:

1. NIST SP 800-53 Guide for Conducting Risk Assessments - https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final

Required people / roles: *CEO, Executive Leadership Team, Information Technology Leadership, Information Security Professionals.*

Day 39-60 – Build A Control Framework

After step 5 you will understand the unique risk profile of your organization. You can now make intelligent, and strategic decisions about deploying security controls. By now you will have a list of controls that need to be implemented of modified in order to reduce overall risk. These controls can fall into any of the five functions established by the NIST Cybersecurity framework.

Some controls are designed to PROTECT you from cyberattacks like firewalls and whole disk encryption. Some controls will be designed to help you DETECT a cyber attacked like Intrusion Detection Systems and Persistent Monitoring. Other controls are designed to help you RESPOND to cyberattacks like Security Information and Event Management platforms or Formal Incident Response plans. Lastly, some controls will be designed to help you RECOVER from cyberattacks such as data backup software and formal Business Continuity Plans.

Step six is where you close the gap that exist between your current state and the desired state that we discussed in step four when you established your baseline. The key is close this gap based on your unique risks. You will have the greatest success in reducing overall risk and eliminating wasteful allocation of resources.

Helpful resources:

1. NIST CSF - https://www.nist.gov/cyberframework
2. ISO / IEC 27000 family - https://www.iso.org/isoiec-27001-information-security.html
3. CIS 18 Critical Security Controls - https://www.cisecurity.org/controls/
4. COBIT - https://www.isaca.org/resources/cobit
5. CMMC - https://www.acq.osd.mil/cmmc/draft.html

Required people / roles: *CEO, Information Technology Leadership, Information Technology Professionals / Engineers / Technicians, Information Security Professionals*

Day 61- 65 – Document And Publish The Cybersecurity Program

Step seven is when you actually document the contents of your cybersecurity program. That's right – document it. There should be at least document:

1. Purpose – where we state the objectives and purpose of the program (*i.e to protect the confidentiality, availability and integrity of data, to reduce operational risk associated with cyber threats and vulnerabilities, to satisfy regulatory compliance requirements*)

2. Information Security Policy Library – where we acknowledge the rules and guidelines that govern our program. It should be a simple listing of the information security policies that have been created (probably during step six – Build a Control Framework) and published to employees.

3. A summary of the Risk Assessment performed to make the program strategic in nature. Include the top risk events and associated responses from management.

4. A summary of our existing control framework.

5. A section to validate our back and recovery preparedness. Acknowledge the existences of good data back up and recovery procedures and document DR testing activities.

6. And section to document future enhancements or improvements to the program – which is typically based on the results of penetration testing and future risk assessments. *Here is what we are doing to improve!*

It is important to have a formal document so that you can share it with your board of directors, superiors, auditors and even employees.

Helpful resources:

1. Cybersecurity Program Template for Download – (enter URL for landing Page here).

Required people / roles: *CEO, Executive Leadership Team, Information Security Professionals*

Day 66- 90 – Test The Effectiveness of The Cybersecurity Program

Now that you have adopted a framework and built your internal control framework you have to validate that the controls are working. An annual penetration test is mandated by many cybersecurity regulations and considered to be a critical element of any respectable cybersecurity program.

At this point in your journey, you have layers of cybersecurity controls deployed throughout your network that are designed to protect the organization from cyber threats. You have a firewall that defends the perimeter of your network. You have passwords that prevent unauthorized access to systems. You have Anti-Virus software that protects your endpoints. These are just a few examples of common controls that exists and are designed to reduce overall risk.

But how do you know the control is working as intended? Are you assuming that they are all working?

Cybersecurity controls are designed, implemented and maintained by humans. And humans make mistakes. Therefore, it is important to test the effectiveness of your cybersecurity controls. This is accomplished by completing an exercise called penetration testing. There are different penetration test types, but they all share a common objective – simulate a real cyber attack. An ethical hacker will attempt to identify vulnerabilities in your technical environment and then exploit those vulnerabilities to gain unauthorized access. This gives you critical insight about where your cybersecurity controls are failing and what you can do to strengthen them.

Have you ever taken two steps from your car only to turn around, grab the door handle and check to see if the door is locked? You are essentially testing that security control. Perhaps you forgot to lock it, perhaps the door was left a little ajar – by checking to see if the door is locked you are verifying the effectiveness of the control.

A penetration test accomplishes the same result for your network environment. How would you know if your firewall was misconfigured? How would you know if there was a machine without password protection? You have to test your controls. Do not assume they are working!

Helpful resources: none.

Required people / roles: *CEO, Executive Leadership Team*

Do Not Procrastinate, Start Now!

In this guide we discussed he eight critical steps it takes to build an effective cybersecurity program and provided a timeframe associated with executing those steps. It is important to take action, do not procrastinate! Understand that once the cybersecurity program is created the contents of the program will have to be periodically revisited over time. Threats and vulnerabilities change which will change your risk profile which may change your control framework and requiring additional testing of new or modified controls. Managing the cybersecurity program will require proper oversight and sponsorship from the Executive leadership team and the outcomes of the steps required to create the program should be revisited as time passes and change occurs.

Go forth and build a great cybersecurity program!

Appendix A: Goal Setting Worksheet

Goal Statement

1. What do you want? Close your eyes and picture what you want with respect to your cybersecurity program. Now give yourself permission to describe this vision below. Paint the picture!

Ideals:

1. *Assurance that the organization is properly protected from cyber threats.*
2. *Confidence that investments made in cybersecurity controls are ACTUALLY going to reduce risk.*
3. *Satisfy regulatory compliance*

2.Define the Mission. What must be done or executed to get what you want? What effort must be expended? What is the next major milestone you must achieve to get what you want?

3.List the Benefits. When you do the work required to get What You Want, what will the benefits be? Why is this worth pursuing? Why would you commit to execution and run through walls to accomplish the Mission?

4.Predict the Roadblocks. What are the things you know, or suspect will impede execution? What will try to prevent you from getting better, from getting what you want?

5.Write the Goal Statement. Goal statements ALWAYS start with the words "I will…"

I WILL *build an effective Cybersecurity Program by (Insert targeted completion date).*

X _____

Signature – It is a contract between you and yourself!