

IDENTIFY, PROTECT,  
DETECT, RESPOND, &  
RECOVER

# FIREWALL



## A BRIEF GUIDE TO BUILDING A RESILIENT LIFE

How to create a personal framework to  
manage risk, adapt to adversity, and  
achieve personal greatness

STEVEN K. GRIFFIN

Copyright © 2021 Steven K. Griffin  
All rights reserved.

This book or any portion thereof may not be reproduced or used in any manner whatsoever without the express written permission of the publisher except for the use of brief quotations in a book review.

Contact Information:

Email: [stevegriffinmail@gmail.com](mailto:stevegriffinmail@gmail.com)

Web: <http://skgriffin.com>

# Introduction

For decades I have spent my life interested in two topics - technology and personal development. I'm not sure when my love for either began, but as long as I can remember I have always had a strong pull toward the study of both.

I grew up in a small town in Central Oklahoma and spent my youth going to one of the larger churches in town. Even back then, I remember having this underlying call toward making myself a better person. At that time, it was religion that guided my path. I would internalize the messages of hope and salvation throughout the week until they became an integral part of who I was. It was during my teenage years that I became serious about intentionally improving who I was as a person.

I graduated high school, went to a few years of junior college, and eventually made my way to Oklahoma State University. When I left for Stillwater, the world opened up fairly quickly. I had the massive university library at my disposal and a whole host of courses I could fill my elective schedule with. I would spend hours just roaming the aisles of the library, looking for books on just about every subject I

could think of.

Even though I majored in Computer Science, I almost always took philosophy classes as electives. It was through these classes that I discovered many of the Wisdom Traditions throughout history. I studied how cultures all over the world have their own ways of expressing what it means to be human and how they each laid out a path for how to better yourself.

I soaked it up.

I learned their similarities. I learned their differences. I learned that throughout the long course of human history, humanity has always had this internal pull and emergence toward bettering itself. Entire schools were built in response to this desire and there have been more books written on the subject of personal development than anyone could count. It's simply a part of who we are.

After I graduated college, I kept up my interest in personal growth by reading books, watching documentaries, and following blogs of various thought-leaders in the space. Over the years, I've tried dozens of frameworks for self-improvement and have slowly learned what methods work best for me. And while I never really found a perfect system, I have been able to take bits and pieces from each and have built a process that has served me well over the years.

That's the interesting thing about personal development - it's *personal*. Everyone has a unique way they are wired. We all

respond a little differently to various processes and ideas. Rarely is there a process that works for everyone. So, I have learned that the key to personal growth is to read as widely as you can and essentially build your own system. One that works for your specific context.

On the other side of the coin, I grew up a child of the '80s when personal computers and the Internet were just coming onto the scene and becoming more mainstream. I can still remember the excitement I had when my parents brought home our first personal computer and connected to the Internet via a modem that binged and bonged as it was communicating with our Internet Service Provider. We couldn't do much with that first machine, but it was enough to spark a head-first deep dive into the world of computers.

I received my first laptop as a graduation gift from my relatives which led me to spend hundreds of hours learning the QBASIC programming language by studying the source code for the *Gorillas* and *Nibbles* games that came with the computer. I would tinker with the code to modify existing gameplay and add new features to the programs.

In college, as I worked through the various computer science courses, I would quietly explore the web of information that was beginning to form online. I remember the mystery and forbidden excitement when I discovered various hacker forums and IRC groups. While in my Junior year, I wrote a software program

to help me aggregate Internet references into a bibliography for various term papers I was writing. I thought the idea was good enough that I started a company around the idea with a few other guys and we eventually partnered with an online education startup out of Oklahoma City where I joined the staff to help integrate the software into the teacher's online curriculum toolkit.

After college, I started a career as a software engineer. From my meager beginnings as a junior developer for the educational startup, all the way to my present position as Chief Information Security Officer (CISO) for a global financial services firm, I have slowly and steadily built my career in technology one brick at a time.

But it wasn't until the most recent chapter of my career, when I stepped into the world of information security, that these two very different aspects of my life crossed paths.

There are all sorts of frameworks in information security that help an organization build a robust privacy and security program with the primary goal of helping an organization manage risk. One of the more popular frameworks is the National Institute of Standards Technology's (NIST) Cybersecurity framework. Early on in my tenure as CISO, I decided that the NIST framework would be the set of guidelines that we aligned our security program with. We would use its principles to structure our path forward.

As my understanding of the NIST framework and its organizational focus grew, I realized that the tools and techniques I was using to cultivate my own personal growth, were no different than what the NIST framework was trying to accomplish - *establish a framework from within which to operate and guide your daily practice.*

The five functions outlined in the NIST framework (Identify, Protect, Detect, Respond, Recover) aligned almost perfectly with many of the practices and routines I was engaging in for self-improvement. I had never codified my routines, I always "just did them." But, the NIST framework put structure and definition to the processes that had helped me achieve so many of my personal goals.

There is a hidden benefit that the NIST framework provides that I didn't realize until I stumbled across a quote by the famous Swiss psychologist, Carl Jung. Jung states, "*The greatest and most important problems in life are fundamentally unsolvable, they cannot be solved only outgrown.*"

When I write a piece of software, I am generally solving a defined problem. Most of the time, I am given an explicit set of inputs, and I am expected to write code that will return a predetermined set of outputs.  $A + B = C$ . And if it doesn't, you know you've messed up. In this way, the success or failure of my attempt can be measured explicitly and definitively.

However, the one thing I quickly learned when I entered the

world of cybersecurity is that there is not really such a thing as a definitive answer or solution.

Nothing is 100% secure.

Ever.

And this is a completely different problem to manage than when you are writing software. Cybersecurity is more about *risk management* than building infallible solutions with definitive answers. You assess the likelihood of something going wrong, try to minimize the chance of it happening, and continually monitor and hone your defense. There is no finish line.

It's a continual process of refinement.

As Jung would say: "*these types of problems cannot be solved, only outgrown.*" The difference here is that rather than having a silver bullet solution to the stated goals of cybersecurity, we have a framework that guides us in methodologies and principles of *continual improvement and defense*. The process of securing an infrastructure is ongoing - you are always adapting, modifying, and upgrading. You are, in essence, adapting to and outgrowing your problems.

I think many times, those of us who are trying to find solutions to our problems in our personal life, quickly become frustrated when things don't come out with definitive answers. We fail to realize that humans are not computers. As such, the pursuit of bettering ourselves will never be as simple as  $A + B = C$  either. Self-improvement is not a straight path. It bends

and curves and requires you to back up, turn around, or occasionally alter your course. Things break. Routines and techniques that work today are not guaranteed to work tomorrow. And much like the world of cybersecurity, it's a continual process of adaptation, modification, and upgrading.

My hunch is that the continual opportunity for disruption, mixed with the lack of tools to manage those disruptions, is the reason that many people find themselves in a state of anxiety. We don't know how to handle the unknown, the unpredictable. We don't know how to manage risk in our lives.

In information security, risk is defined as: *the likelihood that a threat (internal or external) will exploit a vulnerability, resulting in an adverse event that will impact the assets we are trying to protect.*

With that definition in mind, I would argue that risk in our personal life could be defined as: *the likelihood that a threat (internal or external) will exploit a weakness in our lives, resulting in an adverse event that will impact the goals we are trying to achieve and protect.*

It's a subtle difference between what we are trying to protect, but the general idea of risk is the same - the likelihood that something is going to screw up your plans.

Here's the key - you approach security and risk management problems differently than you do programming problems.

In programming, you use *logic* to definitively solve a

problem. Just do X and you are guaranteed Y. It has predictability in its outcome.

In risk management, you use *frameworks* to help you manage a context through continual analysis and proactive and reactive adjustment.

There is no definitive answer. Rather, you cycle through the various activities of identifying what is important, classifying and prioritizing them, making plans to protect them, implementing controls to help ensure that they are protected, continually monitoring the status and progress, responding to any events that attempt to impact them and recover when things go wrong.

Most importantly, this process never stops. And as it turns out, these are perfect functions to outline and guide us when looking at personal development.

When you don't have a framework to follow or are not structured in the pursuit of your goals, then disruptions will have a greater chance of completely derailing your efforts. You drift away from your goals and the lack of discipline comes with hidden costs. Not only do we drift away from our goals, but we also cheat ourselves out of a quick recovery for most things that take us off course.

The objective of risk management activities is to reduce the probability of something unexpected occurring, helping you recover when it does occur, and decrease the level of anxiety

around the process. We may not know everything that is going to happen to us in the future, but taking the time to think through possibilities, developing some initial response plans if something does happen, and doing everything we can to prevent adverse events from occurring in the first place will go a long way in helping us minimize risk to an acceptable level.

And that is the goal of this book - to use the tools of information security to build a structure and a framework from within which we can analyze, reduce, and become comfortable with the risk that is in our life.

## **Our Roadmap**

So, where are we headed?

Every self-improvement system takes you through a familiar process of reviewing where you have been, determining where you are today, mapping out where you want to go, and outlining the steps you will need to take to get there.

The five functions that we are going to explore in the following pages are no different.

In the coming chapters, I will walk you through the five functions in the NIST Cybersecurity Framework (Identify, Protect, Detect, Respond, & Recover) and show you how you can leverage the processes of each domain in your life. We are going to learn how to assess risk and hopefully put enough controls in

place so that you will be comfortable with any unknowns that remain.

One important point - there are no universal answers. What works for one person, probably won't work for another. We all come to the table with different backgrounds, social situations, education levels, interests, and contexts. Rather than give you a bullet-proof answer, my goal is to walk you through a process that will lead you to discover and define the actions and tools that work for your specific context.

I'll warn you now, it's going to be a lot of work. Many people will see the exercises and activities in the next few chapters as overkill, but I promise you the effort is worth it. The ideas and exercises in this book will force you to examine your life at a deep level. It is an intense, focused effort to think about your life and build a plan to ensure that you give yourself the best opportunity to succeed. Even if you throw away your work at the end of this, I believe you will still find value in the exercises.

So, why go through all this effort?

Because, first and foremost, it gives you the tools to help you build the world you want to see exist. By taking the time to go through the exercises outlined in this book, you will be bringing a little order to the chaos around you. By the end of the process, you will have a well-written and thought-out plan to create resiliency in your life that will help you protect the

things you have defined as important. As a natural result, my hope is that these exercises will help you reduce risk and anxiety by building yourself a "north star" to follow when things get tough.

Most of all, the framework outlined in this book will give you a shot at maximizing your potential.

After all, you get one shot at life, make it count.

Are you ready to dive in?

# Identify

Most personal development systems follow a common template - reflect on where you have been, assess where you currently are, and define where you want to go. Commonly, these systems will guide you through a series of writing exercises that have you explore some of the defining moments of your life from the past to see any common themes that have emerged or to look at your current situation and collect all the big picture items that are consuming your time and focus.

The purpose of these exercises is to find trends and to look for a trajectory. Are there any common mistakes that you tend to repeatedly make? Are there certain interests that you repeatedly go back to throughout your life? What value did a certain experience provide? What are the most important lessons you have learned through these events? These types of questions lay the groundwork for building the road ahead of you. You discover your passions, look at your weaknesses, and wrap your arms around your typical mode of being.

In the information security world, we have a similar process by which we take stock of everything within our specific

context. This process is called *inventorying your assets*.

Assets are defined as those things that you hold as valuable or things for which you are responsible.

The reason we perform this exercise upfront is that you can't protect what you don't know exists. Not only that but some things in an organization are considered more valuable than others. And you are going to spend a lot more time, effort, and money protecting and managing assets with higher value.

For example, (we'll be referencing this illustration throughout the remainder of the book) suppose you have two pieces of equipment in your organization - a server and a printer. These are the assets that you will need to protect. However, as you can probably already tell, they are not of equal value. The server that contains all your client's confidential data is often valued higher than the printer sitting in the closet. The server probably costs more, and the information that is stored on the machine is extremely valuable. You will be willing to spend more time, effort, and money to ensure that the server is well protected. If the printer gets stolen, probably not that big of a deal. If the server gets stolen or compromised - very big deal.

I believe that your personal growth strategy is no different. Before you start putting together plans on how to make your life more resilient, it's always a good idea to know what is in your life and to prioritize those things so that you

know where to focus your attention.

In other words, you need to make an inventory of the assets in your life.

So, what are considered assets? An asset in your personal life would be anything you consider of value to you, both past and present, or those things for which you are responsible. This will undoubtedly be a big list. Sometimes it helps to break things down into smaller categories.

Within information security, we typically break assets down into three categories: hardware, software, and data.

Hardware is the physical assets of the company - computers, servers, networking equipment, phones, chairs, monitors, etc. Typically the things you can touch and feel.

Software includes all the programs and applications that are licensed and/or installed across the organization.

Data is the various types of information that the organization stores and utilizes to do its work. This is both public and private information.

Leveraging these three categories, we can establish corresponding groups for our personal growth strategy. In fact, we can map them directly to several aspects of our life in order to give us a holistic view of ourselves. The mapping would look like this:

- Physical (Hardware)

- Spiritual (Software)
- Mental (Data)

Let's take a look at each.

## **Physical Assets**

The Physical category will include, first and foremost, your personal health. I've found in my own life that if I am not taking care of my physical body, everything else suffers. It's helpful to be as objective as possible when focusing on this area. Try to stick with the facts. When examining your health, it's helpful to ask yourself questions like:

- How much do I weigh? Does my weight fluctuate?
- What is my diet like? Am I always yo-yo dieting? How often do I eat out?
- Do I have any illnesses that I am currently dealing with?
- What is my exercise regimen like?
- How much sleep am I getting? Do I need more?

## **Spiritual Assets**

The Spiritual category will contain the rhythms and routines that sustain your day. The best indicator of this

category will be your calendar. When assessing your spiritual assets, it's good to ask questions like:

- Where do you spend your energy and time?
- What routines do you have in place to help ground you?
- Do you automate anything to help make things flow more smoothly?
- What are you doing to help others?
- What obligations have you committed to?
- Are you religious? If so, in what way? What do your religious patterns look like?
- Any personal drama in your life?
- What activities and/or people give you "life?" Which ones drag you down?
- How is your mental health? Are you anxious or depressed?

The key to recognizing things that affect your spirit is to think about those things that direct your mood in one direction or another.

A second part of the spiritual category is to think about all the defining moments in your life - both good and bad. We have all had various people and events in our life that we will forever remember. Include these moments and people in your assessment of this category. What were the details of the event? What lessons did you learn? Write these moments down.

## **Mental Assets**

And finally, the Mental category contains those activities and people that you engage with to continually learn and stimulate your mind. Your job. Your family and friends. Education & continuing education. Hobbies.

- What do you do to learn?
- Is continuing education a priority?
- How do you learn best?
- Are there specific teachers or mentors that you resonate with?
- How much news do you consume?
- What type of books do you read?
- Who do you have in your life to bounce ideas and problems off of?
- Who are your mentors?
- How do you track and organize things?

## **Excercise: Invetory Your Life**

Spend a few hours writing out everything that makes up the context of your life. Be sure to include all three levels

discussed - physical, spiritual, mental. I would recommend you go category-by-category to keep from becoming overwhelmed.

Try to simply free-write whatever pieces come to your mind. Don't judge them just yet (we'll get to that in the next section), but simply write them down to ensure they are accounted for before you move on.

We must look at things as they *currently exist* or how they happened rather than how we wish they were. We'll plan goals in a later chapter, but for now, try to be candid with yourself and write down as honest an assessment as you can. Try to be thorough.

This process will take some time. Depending on how old you are, you may have built up a large landscape of things that you have to manage and that make up the context of which you are the center. The first time I went through this process, it took me several days to simply inventory everything.

The important point here is that you give yourself space to think. Be patient. Examine every piece with care, rather than rushing forward to the next step in the process. The more time you take upfront, the more accurately you will be able to assess what things you can adjust.

If you find yourself getting bored or overwhelmed, sit with those feelings for a while (better yet, make note of them). These are typically signs that you may have too much on your plate. Understanding this now will help you in future chapters.

But don't give up. Commit to sitting down and getting as much of it out onto paper as possible. Once you are finished, feel free to move on to the next section.

## **Prioritize Your Assets**

Once you have built an inventory of assets, the next step in the process is to prioritize those assets based on how important they are in your life.

*All things on your list are not equal.*

Using the example of the server and the printer from the previous section, the server and the printer are not equally valued. The server contains sensitive data that, if compromised, could spell disaster for the organization. The server would have cost us several thousands of dollars and therefore would be expensive to replace. Overall, it would be prioritized as being of high importance.

The printer, on the other hand, is easily replaced and doesn't have any sensitive information on it. Nothing disastrous would happen if the printer suddenly stopped working. So, when comparing the two, the server should be prioritized higher than the printer.

I should take a moment and state something obvious here - prioritization will be based on your specific context. Not to complicate things, but if you are running a store that provides

printing services to customers, maybe those printers are a lot more important than the example I provided above. If you have three printers in your store for customers to use and one goes down, then that's one-third of the value you provide to your clients.

Or maybe you run an advertising business where you heavily rely on printed materials in the services you provide. Again, those printers are going to hold a higher value than if we're talking about an online software company.

The point here is that *context matters*.

And everyone's context is different. Take the time and think deeply about your specific context. Your context will require you to prioritize things differently than someone else.

As a personal example, I have a wife and four children. They are some of the highest priorities I have. Because of this, when I look at the risks I'm willing to take, the sacrifices I'm willing to make, and the focus I put on my relationship with them, I spend a large number of resources and effort protecting and nourishing that part of my life. This is a completely different prioritization context than someone who isn't married or who does not have children would probably have.

This is a good time to think about the values you want to enshrine and uphold. What ideals are important to you? Also, think deeply about the "why" behind the choices you have made. Why is my family one of the most important priorities in my

life? Because at the end of the day, they will be the one thing that is consistent in my life. They will be the ones with whom I will share my life experiences. They are the ones who will see me at my worst. They will celebrate achievements and milestones with me. So it's very important that I spend time nurturing those relationships and ensuring that I do whatever I can to make them the highest assets in my life - which means they get the most attention.

### **Exercise: Prioritize Your Assets**

Before you begin this exercise, stop for a brief moment and give yourself permission to be honest. To be messy. To explore and really express how you feel about each item in your list.

When ready, grab the inventory you created in the previous section and spend a few hours thinking about the value each of the items you have written down holds. Define each asset's impact on your life. Ask yourself some hard questions:

- Why is this person, activity, or thing important to me?  
What value is provided?
- How much effort does it take to properly nourish and protect that asset?
- Is it something that weighs you down? If so, note it.
- What is the impact on your life if it is no longer around.

Try to simply-free write whatever pieces come into your mind.

Once you have defined how each item fits into your life, spend a few minutes prioritizing your list. I want you to make two passes - the first pass, I want you to simply label each asset as HIGH, MEDIUM, or LOW priorities. On the second pass, I want you to then rank each asset in order of importance for each group. Put the most valuable assets at the top and order them from most important/life-giving to least important.

## **Assessing Risk**

Before we move on to the next domain, it's important to dig a little deeper and understand your relationship with risk.

One of the major life lessons that working in information security has taught me is the value of assessing risk and coming to terms with how risk-averse I am about certain things.

Back to our example of the server and printer - in the case of the server, we would probably agree that the server containing sensitive client data is more valuable than the printer sitting on someone's desk (again, context matters, but for our purposes, this is the case). As such, I have prioritized the server to be much higher in value and focus than the printer. The next thing I have to do is assess how much effort

and resources I am willing to provide to ensure that the server remains safe. This is a direct result of how much risk I am willing to tolerate. Sometimes this is called our *risk appetite*.

Risk tolerance is personal. Everyone will have a different risk appetite for various things. And one of the best things you can do for yourself on your journey toward self-improvement is to carefully examine what your personal appetite looks like for the different things you have defined as holding value to you. In the end, your risk tolerance will directly affect how far you are willing to go to protect the things that are important to you.

In information security, we do this through a process known as a risk assessment. A risk assessment is a process by which we look at all the various mission-critical aspects of an organization, define the different types of threats that could potentially impact our operations, analyze the likelihood of the event actually happening, define ways in which we could potentially reduce the impact, and then codify what level of risk we are simply willing to accept.

We won't go through that detailed of a process here, but I do think it's important to take some dedicated time and understand what your risk relationship looks like. Are you someone who can tolerate a lot of risk? Or are you someone who has to have everything go as planned and gets thrown for a tailspin if something gets off course? What is the likelihood of

something actually occurring? What is the worst thing that could happen? How hard or easy would it be to correct course if it did happen? Is it something you can even control? Are there ways to mitigate or reduce the level of risk?

As someone who battles anxiety, I have found this process to be extremely helpful in reducing my overall level of anxiousness about various parts of my life. When you take the time to analyze the worst-case scenario of things, it goes a long way in helping you come to terms with what is and is not in your control. At some point, you have to do some deep soul searching. You have to realize that even after doing everything you possibly can to prevent or deter threats and reduce risk, most things in life will continue to have some sort of residual risk. At this point, you have to be willing to accept what's left. Risk is a part of life.

### **Exercise: Analyze Your Risk Appetite**

Take some time and free-write about your tolerance to risk. Are you someone who has to have everything figured out in advance? Does a sudden course change throw you into a tailspin? Write about the things that make you anxious. How have you overcome these types of situations in the past?

When you are done with your list of assets from the previous section and have finished your risk assessment, schedule some time with a trusted partner or friend and walk

through what you have put together. Let them ask questions about the assessments you have just put together. Give them permission to speak into your life and provide constructive feedback as needed. Make any necessary adjustments.

In the next chapter, we are going to begin the process of setting up boundaries and controls to help you protect the things you have prioritized as being important in your life.

# Protect

*"An ounce of prevention is worth a pound of cure."* Have you ever heard that saying? Or how about this quote from Abraham Lincoln, *"Give me six hours to chop down a tree and I will spend the first four sharpening the axe."*

The key idea in both of these sayings is that a little work upfront will go a long way to prevent problems or make things easier down the road. This holds true in our scenario as well - the more we do upfront, the better off and more prepared we will be in the future.

In this chapter, we are going to take some time and establish a framework to help us protect and focus on those things that we have deemed most important. We are also going to look at ways in which we can preemptively reduce the impact of any adverse events that may disrupt our progress toward our goals. Why? Because preemptive actions and preparing ahead of time reduces risk which, in turn, reduces anxiety.

We will accomplish this through the following process:

- Simplification and minimization
- Defining our guiding policies
- Establishing a set of controls
- Building a recovery plan

Let's take a look at each step of the process.

## **Simplification and Minimization**

One of the best practices you can do in information security is to reduce and simplify your landscape. What that means in practical terms is to minimize the number of devices in your organization and simplify how your network is laid out.

The obvious benefit of this is that by reducing your footprint, you reduce the number of things you have to keep up with. And it's no secret that the fewer things you are managing, the smaller the threat landscape, the lower opportunity for compromise, and the simpler everything is to keep running.

Patrick Henry in his famous book, *Common Sense*, said, "*The more simple any thing is, the less liable it is to be disordered, and the easier repaired when disordered.*"

That works in both technology and life.

Hopefully, by this point, you will have spent enough time compiling and working with the list of things that are important to you that you can take your list of assets and quickly see if anything can be pruned away. Just like when you are pruning a

tree and you cut away things in your life that no longer serve you, it gives you more time and energy to put toward things that give you value.

Not only that, but you minimize the number of things that could go wrong and have a better chance at handling any storms that do come in the future (and they will come).

Going back to the world of technology, maintaining a fleet of 10 servers is a much easier task in both energy and resources than managing a fleet of 100. There is less effort spent keeping those 10 servers running, less effort keeping the software up-to-date which reduces vulnerabilities, and less effort ensuring that they stay in optimum operating condition. To paraphrase Patrick Henry: ten servers are less liable to be disordered, and easily repaired when disordered than a hundred of them.

The goal here is to get things to a manageable level. There will be some hard decisions to make and this process may take a few passes to get the list down to just the essentials, but it is important that we establish a baseline of things that we can optimize and strengthen. Once we have a solid foundation built and running smoothly, we can then approach adding back other items in a more cautious and measured way.

### **Exercise: Simplify and Minimize Your List**

Grab the list of assets and all the analysis that you have

written down in the previous section. Take some time to review the list and cut it down to only the most essential items in each classification.

The goal here is to strip everything away except those one or two things that you consider the highest priority in each area of your life. You can always add things back, but I want you to be ruthless in your pruning until you reach the bare minimum number of assets you believe are your most important things to focus on.

As an example, when I conduct my annual reviews each year, I generally have anywhere from 5-10 goals in each area of my life that I would love to work on for the year. However, I know that the more goals I have, the less focus I can give to each one which reduces the likelihood of achieving them. So, I force myself to choose a maximum of 3 per category. That's it. I keep the other items tucked away in a drawer just in case I run out of things to work on, but I rarely get to any of them because I'm focused on the highest priority items for the entire year.

So, take your prioritized list and start pruning. End up with only a handful of items you believe are the most important in your life right now, the items you want to throw all your effort and focus into making the best they can be. Let those items be your foundation.

## Defining Your Guiding Policies

Now is where you get to dream a bit. You've done the hard work of rummaging through your life, defining your context, prioritizing your assets, and ruthlessly whittling your focus down to just the essentials. Now you get to imagine your ideal state for each of these items. What are your ambitions for these areas of your life? What are the standards and ideals that you want to try and live up to?

These will be our guiding policies or values. In technology, they are the stated objectives for our organization. In terms of your personal development, they are your goals and objectives for your life. They are the "*why*" that underpins your entire trajectory.

The goal of this exercise is to cement the values you are aiming for in your life. Your guiding policies should be driven by your risk appetite. They should be easily understood and most importantly - *written down*.

Your guiding policies will be the statements that you will refer to over and over again as you work toward your goals. They are your North Star that keeps you headed in a forward direction.

Often, they change very little and serve as the baseline upon which you measure and compare your progress. When you are done outlining the various policies, you will have a library of statements that, together, will serve as the blueprint for your

life.

Guiding policies do not necessarily tell you *how* to accomplish your goals (we'll talk more about that in the next section), rather, they are a generalization of the goals and values themselves.

Looking at our example of the server and printer - if I were to define a guiding policy around protecting sensitive data, it might look something like this:

- *"Sensitive and confidential data are the cornerstone of our business. Protecting our client's information to the best of our ability ensures that our clients can trust that we will keep their private information safe, and protects us from unwanted disclosure which would damage our reputation and potentially open us up to liability as a business. As such, any servers that contain confidential client data must be properly protected against unauthorized access or disclosure of data."*

In this example, you see that we start off defining why we want to protect sensitive or confidential data - because it is mission-critical to our business operations. We want to ensure that clients can trust us. Also, data protection helps us maintain a good reputation and protects us from potential liability if the data were to be stolen. Because of these

reasons, we outline in our policy that any server containing sensitive data should be protected.

Notice that we don't specify how it is to be protected. We only state that it must be done. Details on how we will accomplish this will come a little later. For now, we just want to establish the ideal or policy that we want data to be protected.

So, what does this look like for our personal life? We'll use the example of health. If your health is one of your priorities, you may define a guiding policy that says something like:

- *"My health - both physical and mental - is the foundation for everything else in my life. As such, it is important that I maintain appropriate body weight, exercise regularly and eat as clean as I can."*

It's a high-level statement that signifies that a healthy body and mind underpin everything else and therefore hold high importance. As in our previous example with the server, it doesn't tell you what the appropriate body weight should be, what exercises you should be doing, or what food you should eat. It simply gives you a higher-level definition and a small dose of why your health is important.

## **Exercise: Write Your Guiding Policies**

Schedule a block of time to think about, define and commit to writing a library of guiding policies for yourself. Dream big. Set high standards for yourself but ensure that the policies you define are achievable. Be sure to reference your prioritized list of assets that you defined in the previous sections. The policies that you define should relate to those top few things that you deemed most important.

Once you have written out your guiding policies, print them out and keep them together. You are going to use them to define the various controls and strategies you are going to put in place to help you achieve your dreams.

## **Implementing Controls**

This is where we move from theory to practice. Guiding policies, by themselves, are worthless. There are lots of people all over the world who have high expectations of themselves. They may even have written their goals/guiding policies down. But, sadly, the vast majority of those dreams will never be realized because people never put operational and technical controls in place to ensure that they are moving forward toward the goals they previously outlined.

For example, in our earlier discussion about the server

that contains sensitive client data, I may have an information security policy that says something like "A client's trust is the cornerstone of our business. When engaging in a service, clients trust us with sensitive and confidential information that, if compromised, could damage our company's reputation and expose us to potential legal action. Therefore, any servers that contain confidential client data must be properly protected against unauthorized access or disclosure of data." If you'll notice, that's a policy goal, but it doesn't give any directions on how to accomplish that goal. That is where controls come into play.

In the information security world, a control is a *safeguard that is put into place to enforce a policy or reduce risk*.

For example, if it is our policy that client data must be protected against unauthorized access or disclosure of data, we might outline the following controls:

- All hard drives are to be encrypted using AES-256 bit encryption.
- Access to the server will only be granted to users on a need-to-know basis.

In our previous example of the guiding policy related to health, we stated that "My health is the foundation for everything else in my life. As such, it is important that I

maintain appropriate body weight, exercise regularly and eat as clean as I can." To ensure that we are living up to the ideals defined in this policy, we begin by outlining more defined goals and actions. We define our appropriate body weight. We outline how many days we are going to exercise and maybe even what those exercises would include. We define what a "clean" diet looks like.

Controls are the daily, weekly, monthly, and annual routines you establish to keep you moving forward.

Controls are also *measurable*.

Sometimes a control can include bringing in others to help or keep you accountable. Maybe you don't know the first thing about physical fitness. So, rather than trying to come up with an exercise and diet plan all on your own, maybe you enlist the help of a personal trainer to help guide you.

Maybe your goal is to quit an addiction. Rather than trying to do it by yourself, maybe you join a support group so that others can help you overcome your problems.

Another good question for this step is to ask yourself - what can be automated? Maybe your goal is to build up savings and stop living paycheck-to-paycheck. One option might be to set up an automatic process of putting a small percentage of your paycheck into a different account each payday.

The list is endless and as I've already mentioned, the controls you put in place will depend on your unique context.

The key here is to ask yourself more questions like:

- What actionable steps do I need to take daily? Weekly? Monthly? Annually?
- How will I know if I'm making progress (i.e. what are the metrics I should be tracking and how am I going to monitor them)?
- Do I need accountability?
- Do I need specialized training or professional help?
- Are there any situations I need to prevent?
- Do I need to implement anything to help correct me when I get off course?
- How will I know if a control fails?

Controls help limit and minimize risk. Don't look at them as burdens to be fulfilled, think of them as steps toward reducing the possibility of failure.

When you are done with this section, you will have a plan of action that you are ready to begin implementing.

### **Exercise: Define Your Controls**

For each of the guiding policies you printed out in the previous section, take some time to outline what controls you can put in place to ensure you are working toward your goals.

Remember to ask yourself the following questions:

- What actionable steps do I need to take daily? Weekly? Monthly? Annually?
- Can I automate anything to ensure that it happens without me thinking about it?
- How will I know if I'm making progress (i.e. what are the metrics I should be tracking and how am I going to monitor them)? How will I know when I have fallen short and need to adjust?
- Do I need accountability?
- Do I need specialized training or professional help?
- Are there any situations I need to prevent?
- Do I need to implement anything to help correct me when I get off course?
- What type of routine maintenance do I need to do?

## **Building A Recovery Plan**

Things are going to go wrong. No matter how many good intentions you set for yourself, or goals you outline for your life, controls you put in place to keep yourself on track, somewhere down the line things are going to go off the rails.

Count on it. Most importantly, *plan* for it.

You've done a lot of work up until this point to catalog

those things that are important to you, prioritize them, look for threats, build a library of guiding policies and goals that help you live to your fullest potential, and have implemented processes and routines to help you get there. But, protection also means planning for when things go wrong.

In the technology world, we create what is known as a Business Continuity Plan (BCP). The BCP is a document that details the alternative steps you are going to take to bring the business back online in the event of an adverse event.

Most of the time we are thinking in terms of natural disasters, power failures, human errors, outside attacks, etc. This is NOT trying to prevent disruption, that is an impossible task. Rather it is a strategy that is thought out ahead of time to bring the organization back online when a disruption occurs to ensure the minimal amount of disruption and loss.

I can't stress this enough: this is probably one of the most important parts of building a program that is resilient. Having a backup plan is key in ensuring that the goals of an organization are not disrupted beyond what is tolerable.

*Most people don't think clearly when they are in the middle of a crisis.*

So thinking about these things ahead of time, when you are calm and focused, will help give you a reference point to return to help you have a baseline for working your way through a disaster.

And it is the same principle with your personal development and goals. Expect disruptions. If I can promise you anything in this little book it is that the plans and controls you have already put in place will not be enough. Something somewhere will cause your plans to go sideways.

Sometimes the disruptions are small - you get sick and are not able to work out for a week. Sometimes they are huge - your house burns down. Regardless of the size of disruption, one of the best things you can do ahead of time to protect the things you have outlined as important in your life is to take some time to think about contingency plans and those things you can do to get back on track and move forward.

In our server example, some things we might think through in terms of business continuity include defining:

- How and where do we store our backups of the server?
- How often do we test restoring those backups?
- What offsite location will we keep the backups at?
- What is our recovery time objective for getting things back online?
- How much data can we afford to lose without it impacting our business?
- What alternate location can we work from if our office space is no longer accessible?

Essentially, you are thinking through plans and processes (and testing those plans and processes) that will be needed should you be knocked out of line from your normal business operations.

The risk assessments that you created in the previous chapter for your most important assets can be used to guide you in determining what items you should consider creating continuity and recovery plans for.

So, when looking at our personal lives, what should go into a recovery plan? Here are some ideas:

- Emergency contacts and numbers.
- A consolidated library of important documents. Fireproof safe?
- A plan to save some extra cash just in case you have an emergency.
- What do you intend to do if you fall off the wagon and derail progress toward your goal? How will you get back on track? Who will you call in to keep you accountable? What drastic measures are you willing to take to correct the course?
- Outline what tools you will use to help you mentally process the event. Journaling? Counseling?

Keep this simple. Most importantly, write it down. I would

recommend taking your top two or three items and building recovery plans for only them. Then scan through your list and figure out what things you would have the hardest time with getting things back on track and put a plan together for those items.

I know this sounds like a lot of unnecessary work, but this exercise accomplishes two things: first, even if you never break out your written recovery plan, simply by going through the process of thinking about recovery options and putting it in writing, you will see benefits. Think about the defining moments that you listed out earlier that weren't so good. How would you respond to those situations or events again?

Second, you are going through a deep and focused effort to analyze your life. In building a recovery plan, you will have the opportunity to see which items on your list are complicated and which ones are simple to correct. This analysis alone will help reduce anxiety around various things.

I know that in some of my own planning, things that I thought were so important, ended up being very minimal in terms of impact on my life and the effort it would take to recover. My level of anxiety around those items reduced significantly. Remember, our overall goal in this book is to analyze, reduce, and be comfortable with risk in our lives.

The last part of building a recovery plan is to define ways in which you intend to learn from failure. It's not enough to

simply recover from whatever events come your way, the real opportunity for growth is to take the time to analyze the situation and determine how you can improve for the future.

We often call this a debrief or an event analysis session.

We'll talk more about review strategies in a later chapter, but for now, you are simply going to figure out how you learn best. I always recommend writing things down, so my first proposal is to build a process around journaling. Maybe you learn differently and synthesize information by talking through things rather than writing. That's fine.

Define how you plan to codify what happened and the lessons you learned.

### **Exercise: Develop a Plan for Recovery**

Take some time to plan for failure and build a recovery plan. Grab all the work you have done up to this point and review your list of prioritized assets. Starting with the most important ones, look at all the various threats that you defined that could cause problems and consider writing out a plan of recovery.

For each item think about:

- What will be your immediate response?
- Do you need to have outside help? If so, who?

- Are there any documents that you need to note that are important and would need to have handy? If so, which ones? (for example, I have kids...and kids could potentially get hurt and need to go to the doctor. So having our medical insurance cards in a predefined location will help reduce the stress of having to find them at the time the event occurs)
- What tools are you going to use to help you process the event and learn from what happened?

When you are done with your continuity plan, schedule some time with a trusted partner or friend and walk through what you have put together. Let them ask questions about the plan you have just put together. Listen to their constructive feedback and make any necessary adjustments.

I recommend that you take all your notes, organization, and exercises and put them in a safe, but accessible location. You will want to refer to them often.

You may want to go back through everything you have done up to this point and summarize some of the key pieces on a "cheat sheet" of sorts. I like to bullet point all my goals for the year on an index card and keep it with me in my journal as a reference. I'll also write down some of the key controls that I put in place as a reminder of what I've committed myself to do to accomplish those goals. Summarize the key points of your

overall plan to help keep your guiding policies and controls at the top of your mind every day.

At this point, all the planning is done. It's time to start putting our plans into action.

# Detect

Now we move into the day-to-day efforts of detection and response. You've done a lot of work up to this point to get clarity on your life, you've defined some goals and guiding principles, put processes in place to help you stay on track, and have even put a plan in place that defines how you will approach failure. The inventory of your life is accounted for and your playbook is written...now it's time to execute and ensure that you are staying on track.

It would be a tragedy to do all the hard work that you've done only to put all your efforts to the side and attempt to make progress without continual monitoring, oversight, and accountability. This is where the detection function comes into play.

Detection, much like its name suggests, is about implementing routines and processes to continually look for anomalies in your day-to-day that could potentially lead to disruption. It is implementing the tools and techniques that will help you record and analyze the various events in your life to determine if you are running into a problem.

You will always have events in life that occur out of the blue (car wrecks, personal injuries, natural disasters, loss of jobs, market crashes, etc.), but with a little bit of luck, the detection processes we are about to put in place will help minimize or prevent some major (or minor) disasters from happening without you knowing.

Let's take a look at a few techniques you can leverage to stay aware of any potential problems.

## **Logging**

One of the keys to the detection stage is putting a robust monitoring and accountability process in place. The start of this process is to *record* your activities and progress toward your goals. We can do this with a practice known as *logging*.

Logging is foundational to computer security. And, just as it sounds, logging is the activity of recording various activities and events for a particular resource. In our example of the server that contained sensitive client data, we could simply build the server, install all the necessary software, and hook it up to the network and start using it. There is nothing that would prevent the server from performing its designated duties.

But...

If all of a sudden, the server stops responding, or user accounts are no longer working, or we see that our critical files are completely gone, we would have a difficult time diagnosing the problem. That's because we have no indicators or records to look at. Nothing to tell us that certain software was causing errors, or that an intruder somehow compromised a user's credentials, elevated his/her privileges, and locked everyone else out, or that a hard drive was starting to fail.

We would miss potential warning signs.

This is where logging comes in. With logging, we can tell the system to record various activities and events that the system is performing or any errors that occur while it is in operation. We record things like who logged onto a machine, when they logged on, if they changed their user privileges, what files they accessed, the status of various pieces of hardware like the disk drives to help alert us if something is starting to fail, etc. We can even have application-level logs that tell us what individual programs are doing.

All of these logged events give us a record of the overall system's health so that we can start to look for anomalies and hopefully be out in front of any critically fatal events from occurring. They give us a reference point from which we can make sense of the environment. We'll talk about how to use these logs a little later, but the critical point to make right now is that we *generate* the logs for later use.

When it comes to your personal life and the strategies we are putting in place, taking the time to put processes in place to record the various events and key metrics in your life is the foundation of everything else. It gives us situational awareness.

You may be objecting to this idea right now by saying things like "I don't have time to record everything," or "I've never been good at journaling," etc. But we're building a life of resiliency. Resiliency requires that we are continually paying attention to the events of our lives and adjusting as needed. The reason I am putting a heavy emphasis on recording the events and metrics of your life is that it is very difficult to analyze what you don't record.

Okay, maybe that's a little strong, but I would argue that you will have a more difficult time analyzing and are at higher risk to miss something important if you don't have records to look back on. Why? Because our memory is fragile. We easily forget details. Writing down events of your life gives us the best chance at seeing the whole context.

The undeniable fact is that somewhere along the way, multiple times along the way, you are going to go off track. Things will go sideways on you. An unexpected event is going to happen. And when they do, having your log records are going to help you respond to the event more quickly, with less emotion, and hopefully recover a lot faster than if you were just winging

it.

Logging comes in many different forms, and the type of logging that you are going to implement will, of course, depend on the things you have prioritized in your life. Sometimes logging means you need to be journaling on a routine basis. Sometimes it means you need to be recording specific metrics - like if you were training for a race you would record things like date, distance, time, your weight, how you felt, what you ate, etc.

Prioritize it and record as much of your life as you can. I know time is tough to find, but as with anything, if it is important to you, you will *make* time to do it. I urge you to make time to record the important parts of your life. Make the process as simple as possible so that you will have less resistance to writing things down. Take a notepad with you everywhere you go. Use an app on your phone to take notes throughout the day and then transfer them to paper when you get home. Whatever it is, find an easy method and start recording things.

I break logging down into two types: metrics and analytics. Metric logs are simply recording specific measurements - who, what, when, where, date, distance, weight, duration, etc. These are snapshots of data for a specific event or point in time.

Metrics help you see trends over time. They are concrete values that give you a fairly black-and-white way of seeing

progress. The important part is that they are *measurable*. These are the spreadsheets you create for things like your workouts, running logs, how many books you've read, stuff like that. I also consider things like doing your finances each week (i.e. going through your transactions, balancing your accounts, and totaling up your overall financial picture) a form of metric logging. The numbers are what they are, they are measurable, therefore they can be considered a metric.

Analytics is more of an abstract process of recording your thoughts, emotions, and meaning extracted from events. It is where you can record your emotional reactions to these events and try to parse out the wisdom and value you have discovered. Many times, written journals serve as a good way to perform analytical logging. Often, I find it helpful to ask myself some leading questions like:

- What did I learn?
- Did I handle that situation correctly? What would I have done differently if I could have done it again?
- What am I grateful for?
- What do I need to do to prepare for \_\_\_\_?
- Is there anything I need to correct or adjust?

If you are diligent about the logging process, not only will you have a great foundation to begin monitoring and

analyzing your life, but you will also be creating a record of your life. This is one of the unexpected side-benefits that I have come to appreciate about the process. Yes, it is a lot of intentional work. But the fact that I can look back over almost 10 years of records I have created, journals I have written, issues that I have had to work through and have overcome, I have a great appreciation for the fact that I have a record of it all. Maybe my kids or someone else will look back and see how one person lived their life and find inspiration for their own.

### **Exercise: Establish a Logging Routine**

Now is the time to think about what types of logging activities you are going to perform. Think about the items you have prioritized and determine what types of logging they lend themselves to (metrics or analytics).

Once you have gone through your list and decided what types of logging you are going to do, build a template to record your activities and metrics, or select a journaling method. Again, make this process as easy and frictionless as possible. I tend to use Google Docs for my analytical journaling. I use a mixture of Google Sheets and yellow legal pads for recording various metrics like words written on a project or my daily walks/runs.

There is no "right way" of logging. The important part is that you are taking the time to record the events and your

thoughts.

## **Monitoring and Analysis**

As you start the process of recording your activities, you will undoubtedly begin to see patterns and eventually be keenly aware of your habits and tendencies on a daily, weekly, and monthly basis. However, it's always good to establish a *scheduled* review process to look at everything that has happened and try to determine if anything is out of the ordinary, starting to slip, or has gone completely off the rails. This keeps you accountable to the goals that were originally established.

Most problems have some sort of warning sign. To continue our example of the server holding client data, in the previous section, suppose we established a logging routine that records who is logging into the server and when files get added or deleted. That's a great start. But how do we know that only those users who are supposed to have access to the data are the only ones logging into the server? We have the record of the events, but unless we are actively monitoring those records and reviewing them, we may not know about anything until the damage is already done.

This is why we must frequently review and monitor what we are recording. Data without analysis is pointless.

Depending on the specific item you are focused on, there may be ways to set up automated alerts to notify you of anything out of the ordinary. For example, if one of your goals is to ensure that your finances stay within a budget, you may have the ability to set up alerts with your bank or credit card that will notify you when account balances get below a certain threshold or if something is purchased over a specific dollar value. I've been able to stop fraudulent purchases in a short amount of time on my credit card because I had automated alerts set up to notify me anytime my card was used at a gas station (a commonplace that identity thieves will use stolen card numbers). I received an alert that my card was used at a gas station and neither my wife nor I had been out of the house all day. After quickly logging into our account online, we saw that there were additional unauthorized purchases made immediately after the gas station charge. Had we not had the alert setup, there is no telling how many unauthorized purchases would have occurred without us knowing about it. We were able to minimize the damage to just three purchases overall before the card was frozen, stopping all future transactions.

The point here is that there will be some things you can automate and others that you will have to set up a process to review your logs on your own.

When reviewing your records on your own, it has been a favorite cadence of the personal development world to try and

establish daily, weekly, monthly, quarterly and annual review processes.

The process of conducting routine reviews of your life is the glue that holds all of this together. Let's take a look at each, starting with the annual review.

## **Annual Review**

Once a year, it is helpful to take one or two days, preferably offsite and away from your house, to look at the big picture. To give yourself enough time to reflect, dream, and codify what you want to do in the coming year.

It can be any time of the year, but I generally like to do my annual review during the week between Christmas and New Years' day. It doesn't matter what time of year you choose, but the important point is that you carve out dedicated space to reflect and plan at the macro level.

There are all sorts of ways to conduct an annual review. Over the years, I've tried various processes and I encourage you to seek out different ways of doing it. But, here is a basic process to help you get started:

- Schedule Your Review - schedule 1-2 days on your calendar to focus on the review. Preferably, this is done away from your home.

- Review Your Records - start by reviewing all of your various journal entries and reviews from the past year. If this is your first time conducting an annual review, feel free to move to the next step. Review the guiding policies that you previously defined.
- Extract the Defining Moments - as you review your records from the year, make notes of the key moments that occurred. Write them down on a separate list so that you can work with them later. If this is your first time conducting an annual review, or you do not have records to reference, simply think back over the past year and write down the key highlights.
- Write an Overview - take your list of defining moments and write out a narrative overview of your year. Discuss what went well throughout the year and what didn't. Look at your goals from the previous annual review and explain how things went, what you accomplished, or where you fell short.
- Outline Your Goals - turn your attention toward the coming year. Define the categories that you want to work on (health, finances, work/business, family, etc.) and

establish 3-5 goals in each for the coming year. Set goals that lead to the type of life that you want to have and that align with your guiding policies. I find it helpful to take a little extra time and write out a narrative explanation as to "why" I want to accomplish the goals that I have set. For example, here is a short summary of one of my goals to paint our house this year: "Ever since we bought our house, we've wanted to paint the exterior white. This year we are planning on getting that project done. We have the money now and hopefully, we'll have some nice weather this year to get it done. We're planning on doing it ourselves, which I'm a little hesitant about, but I think we can get it done if we plan a week or so to do it. At a minimum, we can get the trim done in a relatively short time (maybe a weekend?). In terms of planning, the Spring is the best time for us to try and get the project done. Therefore, I would like to have the exterior of the house painted by the end of May (5/31)."

One technique that works for many people is to ensure that the goals follow the S.M.A.R.T. pattern:

Specific - Make the goal exact. (ex: "I will lose 20 lbs")

Measurable - able to set daily, weekly, and monthly steps and see progress

Achievable - make it realistic

Relevant - ensure the goal aligns with your guiding policies

Time-bound - set a target date (ex: "I will lose 20 lbs by June 1st, 2021")

- Summarize Your Goals - if you have written out your goals in a narrative form as suggested above, one last step that I find helpful is to extract each concrete goal into a concise, bullet-pointed list. I then transfer this list to an index card that I keep in my planner the entire year so I can see it while planning my days.

## **Quarterly Review**

A quarterly review is a simplified version of the annual review. At the end of each quarter, schedule a few hours to look back and reflect on what you have accomplished and what needs to be adjusted for the next quarter. This process can take me anywhere from 2-3 hours up to half a day.

Here is a basic process to help you get started:

- Review your records - start by reviewing your daily and monthly notes and journal entries
- Write an overview - write out what you think has gone well over the past three months. Where did you succeed? Where

did you fail?

- Outline adjustments - write out what changes needed to be made for the next quarter
- Establish goals for the next quarter

Again, the quarterly review is a miniature version of the annual review. It covers a shorter time frame, but still walks you through the process of reflection and planning.

## **Monthly & Weekly Reviews**

The monthly and weekly reviews follow the same pattern: Overview, Adjustments, Goals. Typically, I like to schedule 1-2 hours for my monthly reviews and somewhere around 30 minutes for my weekly reviews.

After a few years, the review cadence becomes very familiar and the process becomes easier with each iteration. As you go, you begin to build a centralized set of activities and documents for monitoring your life.

I know it seems like a lot, but the goal of establishing a consistent routine and pattern of reviewing your life is to *create awareness*. When you are consistently analyzing your life and planning your next steps, you are more likely to notice when something is out of alignment and what steps need to be taken to correct it, much faster.

A final suggestion - when you complete your annual review, take some time to look at your calendar for the coming year and immediately schedule appointments with yourself to conduct your quarterly, monthly, and weekly reviews. Putting them on your calendar helps make the process a priority. If you wish to conduct your reviews offsite, go ahead and look at what locations you will use and book them, if needed.

### **Exercise: Scheduling and Conducting Your Reviews**

Grab your calendar and set aside some time to schedule your various reviews. Begin with your Annual Review. It doesn't have to be at the end of the year, but pick a recurring point in the year and set aside a day or two to conduct your review. Once you have your annual review scheduled, do the same with your quarterly, monthly, and weekly reviews. Protect these dates and commit to them. They will be some of the most important dates on your calendar.

Adapt the processes outlined above to your specific needs. Be sure that when you are conducting your review that you bring your previous reviews, journals, and guiding policies with you so that you can reference and review them as needed.

I also recommend that once you are done with your annual review (maybe even your quarterly reviews), schedule some time with a trusted friend and go over the document with them. Let

them ask questions and adjust your plans and add any new insights as needed.

## **Updates and Continual Education**

The one thing I love (and hate) about computer security is that there are always new vulnerabilities being exploited or methods discovered for attacking a system. The landscape is always changing. The bad guys are always improving and upping their game. As a result, a robust information security program will always contain some sort of process and method for continual education and updating of systems as well as a process for educating the users.

The second Tuesday of every month is known as "Patch Tuesday." It's when many of the major vendors release fixes for vulnerabilities or improperly working code (they "patch" the holes in the systems). And so every month, thousands of system administrators around the world are busy downloading the updates and applying them to their fleet of machines.

The same thing happens with antivirus software. As I'm sure you are aware, there are bad guys in the world who write programs that are designed to do malicious things on your machine like encrypt your files so you can't access them without paying a ransom, logging your keystrokes, and stealing your passwords to your various accounts, or sometimes even completely

wiping out your system and rendering it inoperable. So, to defend against this type of risk, we put antivirus software on machines to continually monitor for bad programs. But those antivirus programs are only as good as what they know to look for. They have a library of what are called *signatures* that tell them what to look for when scanning for malicious programs. And because the malicious programs are always changing, this database of signatures must continually be updated with new information.

So, that server that contains all our client data should have an antivirus program running that is continually updated with new information on the latest threats that are out in the world. We should be patching the server every month to ensure that we keep the system as resilient as possible while in use.

Your personal development is no different. Sure, having a regimented routine that you follow to work toward your goals and to keep yourself aligned to your personal values is better than nothing, but I firmly believe that the key to any robust personal development system - just like an information security program - is to have some sort of routine or process in place in which you are continually learning and upgrading your skills and knowledge. You should always be looking for new ways to improve - new techniques, routines, habits, etc.

In other words, become a life-long learner. Commit yourself to a life of continual education. Double down on the things that

are successful and adjust the things that are not working.

By committing to ongoing education, you are always adding new tools to your toolbox and continually building a defense against new threats that may enter your life. And just like the routine cadence of "Patch Tuesday" or daily virus definition updates, by setting up a process of continual learning in your life, you will strengthen your resiliency against any storms that come your way.

Some common ways to accomplish this might include reading books, magazines, and blogs. Taking online courses. Joining discussion groups and professional organizations in your area. Meeting other people with goals that are similar to yours and asking each other questions to find out how they do things. Regardless of how you learn, the important part is that you are actively pursuing new information and knowledge to help you make better decisions in the future.

### **Exercise: Create a Strategy for Continual Education**

How are you going to continue to educate yourself and grow? Take a few minutes and make a list of books that you want to read, courses you want to take, seminars you want to attend, etc. If possible, make them relate to one of the areas you are trying to improve in your life. For example, if you are trying to get your finances under control, grab a few books on personal

finance to help give you strategies to accomplish your goal. Ask yourself, "who can I learn from?" Seek out new ways of doing things. Make it a goal to learn something new by a specific date.

## **When Disaster Strikes**

So, you're working on your plan. You're doing your weekly, monthly, quarterly, and annual reviews. You're constantly assessing your situation and keeping your eyes out for anomalies or when things are starting to drift.

All of a sudden, you realize something has pulled you off course. Or maybe you did it yourself. Or disaster strikes. Or something that is completely out of your control shows up and must be dealt with immediately.

What now?

You need a strategy to address such situations as calmly and as objectively as possible. In the next chapter, we will look at the next core function of our plan which is to develop and understand how to respond to incidents in your life that are not a part of your original goals and plans.

# Respond & Recover

One thing is for certain in life - you can have the best strategy laid out, you can follow a plan without fail, but eventually, something will go wrong. No matter how hard you try or how prepared you are, something somewhere will come along and wreck your plans. No one gets out of this life without struggle.

No one.

So, why do so many people float through life without a plan for when they fail. It's like the weather - you can have a lot of sunny days, but eventually, it's going to rain.

No one likes to talk about failure. It's uncomfortable and awkward and requires you to admit that things aren't always perfect. But, if put in the right context, failure can be a catalyst for substantial change in your life. I once heard someone say that just because life doesn't go the way you want it doesn't mean you're going down the wrong path. There's a lot of wisdom in that statement. Because every time you encounter failure or something that impacts your life, you have the opportunity to learn something new that will hopefully give you the chance to make yourself better.

One of the biggest lessons that I have learned over the years is that my response to any sort of unforeseen event or incident in my life will determine how quickly I will recover and be prepared for the next time something happens.

Within information security, we call this process *incident response*. The goal of incident response is to recover systems quickly enough to allow the business to continue to operate. It is the process of identifying, investigating, and responding to an adverse event in a way that minimizes the impact it has on the business.

We know that at some point the server may fail, a harddrive may go bad, the motherboard may blow, or the server may get compromised. The goal in this situation is to try and have a *planned* response before the incident takes place.

Hopefully, some of the work that was done during the PROTECT phase of the process will serve to expedite the response process. If you remember, a few chapters ago we built a Continuity and Recovery Plan in which we thought through all the things that could likely go wrong with our plan. It was a mixture of response and recovery steps that would help us when times get tough.

We often break the incident response process down into three stages: Identify, Investigate, and Response. These three steps, while it seems to be a bit of overkill when reacting to day-to-day events, help us have a more intentional response to

an incident in a way that will hopefully provide value beyond simply fixing the problem.

## **Identify**

Hopefully, by now you have established a routine of logging your activity toward your goals. In the previous chapter, we discussed the strategies of logging various metrics and analytical information for the most important assets in your life. When you do this consistently, you build a baseline of information about your life. You will start to see patterns that you fall into and, more importantly, will have the information you need to know when there is an anomaly.

Back to our server example. Let's say that we've been logging information and we have built up a pattern of login activity on that server. We know by observing the day-to-day logs that people access that server between the hours of 8:00am and 6:00pm (normal business hours). This is done day in and day out for weeks and months without fail.

Then one day you're checking your reports and you notice a login record for 1:15am. Immediately, you know something isn't right. Why? Because you have built a baseline of *expected behavior* over the past months of operation. And when something unexpected shows up - it is a lot easier to spot. If you are reviewing this on a routine basis, you will see the event much

faster than if you wait for something to happen by chance.

So, translate this to your personal development - when you are logging information about your activities toward a particular goal, you develop patterns of expected behavior. For example, I have a pretty standard morning routine:

- 5:00am - Wake up and stretch while my coffee is brewing (usually about 10 minutes)
- 5:15am - Pour a cup of coffee, write a little bit in my journal and work on my current writing project. If I am working on a novel, I can usually write around 500 words during this time. If it's a nonfiction piece, it's closer to 1000 words.
- 6:15am - Change into my workout clothes
- 6:25am - Go for a morning walk with my wife
- 7:15am - Shower and prep for the day
- 8:00am - Start work.

I've done this routine for so long that all my morning activities can be logged almost down to the minute.

But there are days when pieces or my entire schedule fall apart. Maybe I only write 200 words in a morning, rather than 1000. Or maybe I don't write at all one day. Inspiration simply wasn't there and I wasn't able to pull the words out of my brain and onto the page. Or, sometimes my discipline falls short and I

end up opening the news and getting lost down a rabbit hole for longer than I should have. In the context of my life and personal goals, these types of days are considered anomalies. They are unexpected/undesired events that impact the progress toward my stated objectives.

I could have two responses to a situation like this - first, I could simply say "Well, it was just a bad day. No big deal." and move on. Pretend that the incident never happened and hope that I can get back on track the next day. But, what I've come to realize is that if I ignore incidents like these and do not take an active response to them, they will repeat themselves more frequently. One day quietly becomes two. Two days become a week. And before you know it, I've gone several weeks and have only written a few hundred words.

Or, I can immediately look at the lack of work I've done and recognize the event for what it is - an anomaly in my daily routine that could potentially spiral out of control. More importantly, it is an event that usually requires me to take action and respond in a corrective way.

It is important to reiterate that this process of detection becomes a lot easier when I am recording my daily activity. I generally have a metric log where I am recording my daily word count on a project, and an analytic log (journal) where I am writing out my general mood, concerns, and thoughts for the morning. Between these two logging mechanisms, I can usually

tell pretty quickly if something has gone off the rails and needs to be corrected.

## **Investigate**

So, what happens when you detect something is off? Many times, our first instinct is to try and immediately correct things. But while that may get us back on track and moving forward again, sometimes an instant response to fix a situation hurts us in the long run.

What I would like to advocate for here is not necessarily a slower response to an event, but a more deliberate response. Rather than just simply fixing whatever is broken, it is often worth the extra effort to investigate the situation and its context, evidence, and scope before you take corrective action. Why? Because sometimes context matters. Sometimes you need to preserve evidence. Sometimes you need to understand the impact of the event. We want to set up a system that allows us to be intentional about how we address a problem.

When investigating an unexpected event or anomaly, it is helpful to ask questions like:

- Is this event still ongoing? What do I need to do to stop it from continuing? (This is also known as containment)
- How far away from my baseline have I drifted?

- Is there something that triggered this event? If so, what was it?
- Were there other people affected?
- What is the scope of the event? Is it contained to just one particular goal/area in my life or does it cover a larger group?
- Do I need to bring in any outside help to assess the situation, help correct the situation, or provide support in any other way?
- How long do I see this event lasting? Is there a way to reduce the impact?
- Is there any evidence I need to collect?

Not every situation will lend itself to the opportunity to take a step back and investigate. Some things need to be addressed immediately. But, when looking at the priorities in your life and the various goals and policies you've outlined for yourself, most things in life lend themselves to a more measured response than we often give them.

In the beginning, taking the time to write out the details of an investigation is helpful to build the habit of acknowledgment and analysis. You may be able to slowly move away from such in-depth review after some practice, but the act of writing things down helps get things out of your head so that you can look at them more objectively.

## Response

So, you've analyzed the event, collected any evidence, decided whether or not you need outside assistance, and pulled together as much information as you can about what has happened. Now is the time to correct or address the issue.

When responding to an incident, it is often helpful to think of things in three stages:

- *Containment* - limit the damage caused by the incident
- *Eradication* - remove the threat
- *Recovery* - bring yourself back to your baseline or a new normal. Put additional controls in place to help prevent the incident from happening again.

We'll talk about recovery in the next section, but for now, it's important to point out that an effective response will almost always contain or eradicate whatever issue has infiltrated your life.

Containment involves the attempt to stop whatever is impacting your progress and prevent it from causing more damage than it already has. In our server example, suppose that we discover malware made it onto the machine. There are several courses of action that we could take, but an initial step would

be to isolate the machine from the rest of the devices on the network. This would help contain the malware to just one machine, rather than allowing it to spread to other devices.

A good example of this is when I get injured while training for a half-marathon or something similar. My guiding policy is to maintain a healthy body. The controls I have put in place are to run several times a week, stretch in the mornings, and eat as clean as I can. But there have been training cycles in which I would end up injuring myself somewhere along the way. One of the worst injuries I've experienced is Achilles tendinitis. I was running hills one year to prepare myself for what I knew would be a hilly race and ended up with a very sore Achilles tendon. My first response was a bad one - I continued to train.

The pain got worse the more I ran. Eventually, I had to take a step back, do some research, and properly address the situation. In this case, the first thing I had to do was *contain* the problem - i.e. stop it from spreading and causing more damage than had already occurred. So, I stopped running.

It was only at that point I could start the process of eradication - taking actions to remove the threat completely. In this case, eradication meant several things. It meant I had to stop running for several weeks so my Achilles could heal. It meant I had to stretch every day. Rather than going back out and starting to run again, I had to slowly work my way up from a walk to a jog and then to a run. Once I started running, I had

to stretch a lot more deliberately before my runs and I had to pay better attention to my pace and form when running hills.

All these things worked in conjunction to remove the threat of my Achilles from flaring back up and causing me problems again. It's a simple example, but one that provided a foundational lesson to me that sometimes you can't just power through and pretend an adverse event never happened. Sometimes you need to slow down, take a step back, evaluate the situation, and take intentional steps to correct the problem.

The way you respond to a situation, in many ways, is everything. As I said in the beginning, it's not a matter of if something will go wrong, it's a matter of when. So, taking the time to think things through and respond appropriately will determine how quickly you get back on track and continue your work toward your goals.

## **Recover**

Now that you've identified the problem, investigated the context of the incident, the last section we will look at is how to get back on track and establish a discipline of debriefing after an event to ensure that lessons are learned and adjustments can be made.

Hopefully, you had a chance to lay out steps in which to bring whatever situation you are facing back in line with your original goals. Now is the time to execute those plans and take

the first step toward recovery.

The goal of the recovery process is to restore those things that were impaired by the incident. It is realigning or recalibrating those assets that were taken off track and away from your original goals. Often that means taking the actions necessary to get back to the previous routines and processes you were originally working with. Sometimes that means you have to adjust your original plan because the incident was big enough, or exposed a new weakness that you didn't know existed, that it is not in your best interest to return to the way things were. You need a *new normal*.

The investigation process you went through in the previous section will help you determine what actions need to be taken. The important part here is that regardless of whether you are realigning or recalibrating, you must take action to get yourself back into a protected state.

A critical aspect of the recovery process is *time*. It doesn't do you any good to let something drag out for a long time. The longer you wait to recover from something, the less likely you are to actually follow through with it and get back on track.

We've all seen it. One example from my own life in which I tend to drag things out for too long is after I run a long-distance race. I spend months and months training for the event, I run the race and reach my goal, but then I have a tendency to

stop running once the race has come and gone. I always tell myself that I'll only take the week following the race off. But one week becomes two. Two becomes three. And before you know it, I've gained fifteen pounds and haven't run a mile in over six months.

I failed to recover promptly. It's not that the plan or the intention wasn't there, it was that I didn't follow through on the *action*.

Maybe you are trying to stop a bad habit. You've gone several weeks or months without a drink or a cigarette. But then you slip up and give in to the temptation. How do you react? What should your response be in these situations?

My suggestion is that rather than sit and beat yourself up over the problem, you take immediate action. Immediate action helps reduce the impact of the incident. Maybe you call a friend and talk it through with them. Maybe you grab your journal and write down your immediate feelings about reverting to an old habit. Whatever the response is, the important point is that you do not let the event go by without addressing it. Face the incident head-on, immediately.

One strategy you can use as a response is to go through a debrief and feedback process after an incident occurs.

## **Debriefing and Feedback**

It's important to learn from your mistakes or any missteps that happen along the way. Just like in information security, the landscape is always changing. That's why I said in the beginning that this is a continual process that requires constant adaptation and adjustment.

Debriefing is the process by which you take a step back and reflect on an incident that has occurred. It is the deeper investigation into what happened with the expectation that you will emerge with some sort of lesson(s) learned. Sometimes that means you realize you need to adjust your process. Sometimes that means you need to add something. Sometimes it means you need to stop doing other things. Sometimes it means you need to change your goals.

In many ways, the debrief process is similar to investigating an incident when it first occurs, but now you have the luxury of being on the other side of the event and will hopefully have some more objective distance from the situation. It helps to ask questions like:

- What was the root cause of the incident? Was it preventable? If so, how?
- Do I need to implement new guiding policies or controls?
- Do I need more accountability?
- Should I be logging anything that I am not currently logging?

- Should I monitor this process or part of my life more?
- Do I need to update anything related to my recovery plans?

Hopefully, these types of questions and investigations can be integrated into the review process we discussed earlier. This is exactly the type of questioning and reflection that I hope you will be doing during your weekly, monthly, quarterly and annual reviews. We didn't cover it in the previous chapter, but I find it helpful to bring my written debriefs to my monthly and quarterly review sessions so that I can analyze them at a higher level and adjust my plans as needed.

Sometimes you need someone from the outside to take a look at a situation and give you third-party feedback. You become too close to your own processes that you become blinded by them and the only way to get a good look at what needs to change or how to address a situation going forward is to leverage the help of an outside party.

Recovery is often a team effort. Just look at some of the more famous recovery programs. They leverage the power of support groups to help people recover from more serious addictions and issues in their life. The fact that they have helped so many people is a testament to the fact that the idea behind a community of supporters listening and giving feedback in your life works.

Depending on the incident, take some time and think about

whether or not you would benefit from bringing in someone to help you look at the situation with fresh eyes. Maybe they can help you see things that you originally missed. Maybe they can help you determine if the solutions and corrections you put in place during your response were appropriate. Maybe they will give you ideas for the future that you never really thought of on your own.

### **Exercise: Reviewing an Incident**

Take some time and look at the last one or two incidents that derailed your progress toward one of your major goals. Analyze the incident for possible lessons that you can extract from the event. Ask yourself questions and write down the various things you would do differently the next time a similar event occurs. As a reminder, some questions you may ask yourself include:

- What was the root cause of the incident? Was it preventable? If so, how?
- Do I need to implement new guiding policies or controls?
- Do I need more accountability?
- Should I be logging anything that I am not currently logging?
- Should I monitor this process or part of my life more?

- Do I need to update anything related to my recovery plans?

If the situation warrants it, find someone to share your response and review with. Permit them to speak freely about what they would do differently or add any additional insights to your analysis.

# Conclusion

We've come a long way in a short time. If you are still reading at this point, I have to assume you've done a lot of work through the implementation of the various exercises throughout the book. If you took the time to do the work, I do not doubt that you have a great foundation and framework from which to make progress toward your goals.

Nothing is perfect. And I don't claim the framework outlined in this book will solve all your problems. Going back to Jung's quote at the beginning of the book:

*"The greatest and most important problems in life are fundamentally unsolvable, they cannot be solved only outgrown."*

There will be some situations that will not have answers. But, I hope the strategies outlined in this little book will at least give you a few tools to help you build your program of self-improvement.

Feel free to take the steps outlined in this book and customize them to your context. Just like no two technology

environments are the same, no two people's lives are the same. As such, it is expected that your process and routines will be different from mine. The key is to do the work. Put in the effort upfront to define those things that are important to you. Prioritize them. Define how you are going to protect them. Establish controls and guidelines that will help you keep making progress toward becoming a better person. Expect and plan for failure. Learn how to intentionally respond to adverse events that show up and derail your progress and build a robust routine of recovery to get yourself back on track.

If you take the time to think this deeply about your life, I can promise you that you will see results.

Most of all, have fun. I'll be the first to admit that too much rigidity in life can be just as depressing and oppressive as not having a plan at all. Use the framework outlined in this book as a guide and a tool to help you move forward, but don't let the process become something that creates a new choke point in your life. Allow yourself the freedom to work and adapt within its tenants. If something doesn't work for you, change it. Whatever process you end up landing on, find a balance that works for you.

I hope this little book has been helpful. Most of all, I hope that it has helped you unlock a process that will be the catalyst to move you toward building a better life. I wish you all the best. May the framework of identify, protect, detect,

respond and recover help you build the life you deserve.

Go get 'em.

## About the Author

Steven K. Griffin is a husband, father, writer, and homesteader who lives on a small farm near Tulsa, Oklahoma with his wife and four children. He has worked in technology for over 20 years and currently serves as the Chief Information Security Officer (CISO) for a global financial services company.

You can connect with him online at <http://skgriffin.com>.

If you would like notifications on project updates and new book releases, you can subscribe to his newsletter at:  
<http://skgriffin.com/newsletter>.