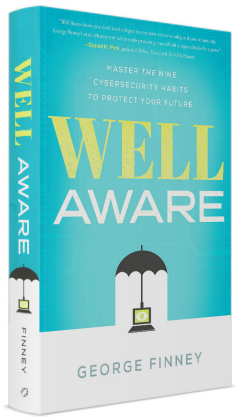
Technology

soundview
Executive Book Summaries®

Well Aware

Master the Nine Cybersecurity Habits to Protect Your Future



by **George Finney**

Contents

THE SUMMARY IN BRIEF

Close your eyes and think of the word *cybersecurity.* Nine out of ten people think of something like a dark room with a number of computers with blinking screens, someone in a hoodie or a mask, trying to scramble through some code as if stealing something. But cybersecurity is about so much more than this. It requires nine powerful pillars that won't just make your organization more secure, but will also help you be a better leader and community.

Each of the nine cybersecurity habits found in ***Well Aware*** builds on the previous one to form a shield you can use to protect yourself, your organization, or your community. The internet is always evolving, so to stay literate, you must continually relearn your environment. And you must understand the best way to educate yourself, your family, or your business. Effective security requires a level of deception without giving up on the community and culture that matter most.

IN THIS SUMMARY, YOU WILL LEARN:

- How to build a comprehensive approach to cybersecurity that incorporates and build on the main pillars of effective security.
- How leadership plays an essential role in cybersecurity and in success generally within your organization or community.
- How security literacy, skepticism, vigilance, and secrecy are critical to cybersecurity.
- The role that community, culture, mirroring, and deception have to play in building a robust cybersecurity plan.

Published by Soundview Executive Book Summaries® (ISSN 0747-2196), 2 Christy Drive, Suite 302, Chadds Ford, PA 19317 USA. • Subscriptions start at $99/year. To subscribe, visit summary.com. • July 2021 • Order #43SS07C Meghan P. Kozak, Editor-in-Chief • Kylie Waytuck, Graphic Designer

Introduction

An element of security involves understanding your environment. This involves continuous learning. Being a skeptic is also important, as it means not trusting something until you've established its credibility, which also requires patience. Vigilance is a state of mind that's about keeping watch so that when you see something, you are ready to recognize it and act.

Secrecy is the natural barrier between that which is public and that which is private. But security and secrecy controls in and of themselves are not enough for protection. Once you've developed security routines, you need to have a plan for orchestrating how those routines work together. When groups of people form, norms are established. You need help to be secure. We work together to solve problems. We share information to protect others and unite in a common defense.

When a company experiences a breach due to a failure of the human element, it's because one or more of these layers of the shield was weak or missing. These nine habits are just as relevant for the programmer coding the next great app as they are for the soccer mom who just wants to protect her kids online. They are just as relevant for the former law enforcement computer forensics investigator as they are for the business executive who is moving his organization into the digital age.

Security is not a technology problem. Sometimes, people make the mistake of believing technology is the most important part of any security program. It isn't. People are the most important part. People use the technology, and people create and implement the processes. To be successful, you can't simply be reactive to threats in your environment. You must identify and proactively change the behaviors that most commonly lead to security challenges before you've been hacked or breached. The result is that you'll be able to use these habits to make your own organization both more secure and more successful.

If you can master the pillars presented in this book, you'll be able to protect the future of yourself and your community.

Literacy

An element of security involves understanding your environment. This involves continuous learning. You need to know how your alarm system works, how to set privacy settings, and what kinds of scams to be on the lookout for.

Literacy also means being aware and making informed decisions.

We don't need to think about security all the time. Instead, we need to have just-in-time security. We must be able to recognize when security issues have come up or are about to come up, and we need to be able to do something about those issues. This process aligns with the definition of literacy.

If being literate means recognizing the words on the page, then having cybersecurity literacy means recognizing potential threats. You may need to have experience to know what to do or how to respond, but maybe you'll just need to Google the answer. The habit of cybersecurity literacy means you have the foundation necessary for seeking sources to find answers and solve challenges.

Skepticism

Missouri calls itself the "Show Me State" because residents won't believe anything unless they see it with their own eyes. Being a skeptic means not trusting something until you've established its credibility, which also requires patience.

We must all be willing to stand up and be 'no men' and women, and it may even help us be more successful in our careers. Still, it's one thing to be skeptical and speak up if the situation calls for it. But when it comes to security, one of the most commonly expressed feelings is that people should be skeptical all the time at the same high level of intensity. But humans should bring the right amount of skepticism with them based on what the situation calls for—no more and no less. This is the habit known as vigilance.

Vigilance

Vigilance is a state of mind that's about keeping watch so that when you see something, you are ready to recognize it and act. Monitoring server logs and reviewing physical access records are great examples of this. Vigilance is a kind of directed skepticism toward specific threats.

One of the first questions leaders ask during an incident is, "Who is this attack coming from?" Often, cybersecurity practitioners don't have the answer to that question. When they do, it often leads to tripled security budgets. But not everyone has that option. Still, whether you have an unlimited budget or no funding at all, the most common path that everyone takes is to start with matters to you or to your organization.

As leaders, our job is proving to our employees how good they already are, how good they can become, and how much capacity they have for being great.

Secrecy

Secrecy is the natural barrier between that which is public and that which is private. This barrier is a healthy part of every human experience. It is so integral to our society that it is a guaranteed protection in the US Constitution's Bill of Rights. The controls we use to protect ourselves are dictated by the nature of the secrets that require protection.

But with secrecy comes a delicate balancing act: Where that barrier falls can change depending on what the secret is. The government might classify one piece of information as top secret, while another piece might only be confidential, and others might be public. This approach has the benefit of focusing your protections on the highest levels of secrecy while also allowing individuals inside the organization to freely communicate about less secret information, facilitating collaboration and increasing productivity. Still, if you have something people think is particularly valuable, you should expect that they will try and steal it.

Culture

Security controls in and of themselves are not enough for protection. When groups of people form, norms are established. Sometimes, these norms are antithetical to security. In these cases, one person changing their behavior won't change the whole company. A culture of cybersecurity embraced at all levels of a company, government, or community is needed.

Cybersecurity culture is only one facet of an organization's overall culture; it must be considered part of a larger whole before it can change. For example, a company may have a high-pressure culture where employees are expected to respond to an email instantly. What hope is there that they'll identify and respond to red flags and phishing messages if this culture is in place? On the other hand, what if the industry or the job is so competitive that changing that aspect of the culture would mean going out of business? Cybersecurity culture should be tightly integrated into company culture as a whole, and the way they interact must be understood.

Diligence

Once you've developed security routines, you need to have a plan for orchestrating how those routines work together. After you've experienced an incident, you must have plans and protocols for handling the way you respond.

Diligence is the habit of taking time to think. When we practice cybersecurity diligence, we plan for what to do when something goes wrong. We prepare for many kinds of events depending on who we are and what we're trying to protect, which requires that we understand secrecy and we know what controls we can put in place to protect ourselves. Cybersecurity diligence includes having a plan in place that we revise when necessary, learning from our mistakes, implementing the right kind of training, and being proactive. When we are diligent about cybersecurity, we take the time to think.

Community

You need help to be secure. We work together to solve problems. We share information to protect others and unite in a common defense. We must look for help not just from law enforcement or inside our companies but from peers in our industry or in similar roles across industries.

What if our job as leaders isn't to coerce our employees into blindly complying with the policies we write for them but creating experiences where they develop the confidence to set their talents free and pursue their potential? As leaders, our job is proving to our employees how good they already are, how good they can become, and how much capacity they have for being great. The foundation that this potential for success is built on is a community of people willing to work together for their mutual protection. This approach requires us to create a culture of cooperation, where it's okay to tell our stories, where we're not shamed for making mistakes, and where we can ask questions if we're not sure what to do. That's the power of a community.

Mirroring

An element of curiosity is involved in mirroring. You want

to be able to see yourself and what you look like from someone else's perspective. Penetration testing is this habit put into practice, but so is looking at your social media profiles from different perspectives or googling your own name.

As you participate in a community, you need to practice mirroring both for yourself and for the communities you are a part of. You'll need to understand what information you may be inadvertently leaking and, through mirroring, change it. You'll play a role in helping your community see itself and improve as well. Ultimately, however, not every leak can be patched. Some doors must stay open for good reasons. The previous habits discussed in this book have shown you how to protect those open doors. We should expect, however, that some small fraction of the people that walk through those open doors will come with knowledge, the ability to evade our defenses, and the intent to do harm. This leads to the final and perhaps most controversial habit: deception.

Deception

Have you ever seen a movie where someone asks a question like, "Do you know Captain Harris?" When the person answers, "Yes, of course!" you know they're lying because Captain Harris doesn't exist. You might create 'lies' in cybersecurity that you use for common password challenge questions. Or you might set up a 'honeypot,' or a security mechanism on your internal network to alert you if anyone accesses it. Deception can be both a preventative and detective habit.

Practicing a handful of deceptive techniques like decoys, breadcrumbs, or watermarking can help you protect yourself and your communities when no other security habit can. This explains why police selectively leak clues to the press to identify imposters. Deception can be an important tool in your arsenal of cybersecurity habits, but it should be used with caution and should only be used as a supplement to all of the other habits.

Deception is not a replacement for the other habits; it complements them. Deception helps you know your adversary and allows you, assuming you've mastered all nine cybersecurity habits, to engage them on terrain where you have the advantage.

Conclusion

Having read this book makes you part of a community. / community is the most important of the nine habits. A security community is a collaboration between a league of community members to protect their common interests. Because security requires a community, and communities arrange themselves in hierarchies, different relationships tend to form with different security implications.

The changes you make in your security will have an impact on all the members of your community, and when they also begin to change, there will be a multiplier effect as small improvements ripple through your shared community. The requirements for this are communication and trust, even if only within a small inner circle. The more openly you discuss security, the greater the impact you will make.

George Finney is the CSO for SMU in Dallas, Texas and is the author of the book, Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future. Finney is a CSO that believes that people are the key to solving our cybersecurity challenges. As a part of his passion for education, George has taught cybersecurity at Southern Methodist University and is the author of several cybersecurity books. Finney is an attorney and is a Certified Information Privacy Professional as well as a Certified Information Security Systems Professional and has spoken on Cybersecurity topics across the country.

Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future by George Finney