CHAPTER 9

The Seven Habits of Highly Effective Security

In our experience, managing security effectively takes not only the right mindset but the right habits, practiced regularly. For instance, some organizations (and to an extent basic human nature) are reactive, and in the case of cybersecurity, it often gets more attention after a recent incident or breach. With cybersecurity, there are always new and evolving threats. Organizations that lose focus, becoming lax in applying the right habits regularly, can more easily fall prey to attackers and even a public breach. The contrary is also true—by applying the right habits regularly, an organization can continually minimize the probability of a breach.

In *The 7 Habits of Highly Effective People*, Stephen Covey\(^1\) sets an approach for personal achievement and improvement based on timeless principles. Instead of focusing on quick self-help fixes and shortcuts, in his seven habits, Covey identified enduring principles that produce long-term results. We adapt Covey’s approach to apply it to the habits of highly effective security.

\(^1\)Covey, S. R. (2020). *The 7 Habits of Highly Effective People: Powerful Lessons in Personal Change* (Anniversary ed.). New York, NY: Simon & Schuster.
In this chapter, we have not only brought to bear our experience but also our consultations with many CISOs and technology leaders. We present the seven habits of highly effective security and discuss how these collective habits help organizations excel at managing security risks. Our primary aim is to share a security mindset in the form of habits. The seven habits of highly effective security are not meant to be a simple, one-time checklist, and the habits mindset needs to be cultivated so that it can apply to your unique environment. By definition, these habits are meant to be broad. We recognize that security programs are not one-size-fits-all and have their own complexity and uniqueness based on the organization which they are meant to support.

As Ben Horowitz once wrote about running companies in *The Hard Thing About Hard Things*,2 “That’s the hard thing about hard things – there is no formula for dealing with them.” We hope that our advice and experience can help with navigating the hard things about managing security risks in your organization. Although there is no one exact formula for achieving cybersecurity excellence, there does exist a combination of art, science, and engineering that can come together to achieve security. Some of the habits we discuss in this chapter focus on the art (e.g., Habit 1 of being proactive, prepared, and paranoid), whereas others (Habit 5 on measuring security and Habit 6 on automation) focus on the science and engineering aspects of achieving security.

Covey’s original book on the seven habits was originally published in 1989. The principles based on experience and research covered in the book are still just as relevant today as when the book was first published, timeless and universal. Although the cybersecurity field seems to sometimes change almost by the minute, we believe that the seven

---

2 Horowitz, B. (2014). *The hard thing about hard things: Building a business when there are no easy answers*. New York, NY: Harper Business.

196
habits of highly effective security are enduring and not tied to any fad or a specific tool promoted by the hottest security vendor at any given time. In these habits, we have attempted to apply the same rigor of distilling key principles that have helped us lead our respective organizations through tumultuous times as well as periods of high growth (Table 9-1).

Table 9-1. Seven Security Habits of Highly Effective Organizations

| Seven Security Habits |
|------------------------|
| Habit 1. Be proactive, prepared, and paranoid. |
| Habit 2. Be mission-centric. |
| Habit 3. Build security and privacy in. |
| Habit 4. Focus on security first; achieve compliance as a side effect. |
| Habit 5. Measure security. |
| Habit 6. Automate everything. |
| Habit 7. Embrace continuous improvement. |

**Habit 1. Be Proactive, Prepared, and Paranoid**

In Part 1 of this book, we covered some of the largest data security breaches and privacy failures that have occurred in many organizations. Some of these firms were technically sophisticated, with investments reaching billions of dollars in technology spend. It is no wonder why so many managers and, by extension, their organizations are feeling helpless against the onslaught of security threats from well-known as well as emerging threats. However, we believe that being proactive, prepared, and paranoid will help ensure that you are in the best position to either discourage an attacker from making you their next target or to reduce the “blast radius” of a breach.
Be Proactive: Act or Be Acted Upon

There are a number of actions that you can take now that will put you in a much better position than waiting for an incident to launch you into action. There are two choices or postures that you always have available to you. Act and take control of your organization’s security by being proactive, or become a reactive, complacent organization that gets acted upon by hackers, compliance requirements, and regulators. When your organization is in the posture to act, it empowers you to prioritize and identify what’s most important first. Proactivity enables greater focus and disciplined execution. Proactivity gives you the upper hand in assembling the most talented resources you can find—both external and internal.

The proactive posture of acting also produces the best return on investment (ROI). Proactively working with vendors to purchase security software services when not under pressure will often lead to (1) better pricing, (2) better and more capable resources to support the implementation, and (3) a better implementation that will help you achieve the results from the investment faster.

On the other hand, when you’re thrown into the acted upon posture, you’re caught off guard and on your heels. When not executing from a position of strength and clarity, suboptimal results surely follow: projects are executed out of sequence, more time is spent on rework, and abandoning earlier investments altogether. All of this leads to higher organizational thrashing, more spending, and less overall strategic value.

Based on our experience, the cost impact of being reactive vs. proactive can be extremely high, sometimes by a factor as much as 100 times. Reactive “emergency” security work is almost always far more expensive than a proactive and planned project. In one example, a standard penetration test can cost three times or more the normal fees and may need to be done in an accelerated fashion to support a client.
request instead of conducting a penetration test that can be confidentially shared with select clients when needed. The time to perform a meaningful penetration test is not when the client is holding the purchase order until the results are cleared with their security team. With rushed execution, one may also wonder if the penetration test is just thorough enough to meet a client timeline instead of done with no immediate client facing deadline. And well before relying on a penetration test, the best way to ensure security is to design it into software. Conducting architectural risk analysis prior to and as software is getting built, with both automated and manual code reviews is a better approach. Consider avoiding the posture of being acted upon as much as possible and minimizing the time spent in that zone.

**Train Employees Continuously**

The most proactive and prepared companies engage in ongoing training, education, and development of their workforce. In-depth training is important for information security personnel, and awareness training is important for all employees, contractors, and third-party partners. We also highly recommend that all developers are continuously trained in secure coding practices and are updated on emerging threats. For information security personnel, it means doing more than sending your two smartest engineers to Las Vegas to attend the *Black Hat* security conference each year. For all employees, engaging in anti-phishing training and ongoing simulation will pay dividends in reducing risks and falling prey to tricks, especially if your organization has not deployed multi-factor authentication or hardware token–based authentication (e.g., YubiKey). Creating awareness and having fun with the training can help reduce the trove of dollars going to scammers using classic “Need help sending an urgent wire” or “Can you do me a favor” emails sent disguised as coming from your CEO.
We want to emphasize and encourage you to train all of the human capital that runs your company, regardless of their employment status or relationship with your organization. We have seen too many third-party providers get compromised and impact the organization they support. For example, if one of your key partners falls prey to a phishing attack that leads to a major ransomware situation, you may end up feeling the pain just as much as your partner who is the primary victim. Training and ongoing education should also be tied to rewards. Consider highlighting and recognizing teams and individuals.

- Which department is most engaged and has high scores for not clicking phishing links?
- Which scrum teams have completed their secure coding training?
- Which teams have the least amount of security bugs to fix or the fastest speed of closing said vulnerabilities?

Executives need to see these results and understand their team’s readiness as well as their progression.

**Proactively Build and Maintain Your Support Network**

Security and technology leaders need to be proactive about having a support network of other professionals outside the firm that they trust and collaborate with. Proactively building a powerful support network is valuable and should be something you invest in. While it does not require a financial cost to continuously build and develop an external support network of peers and advisers, it requires an investment in time from leaders at all levels. It also requires that you add value and help others to nurture the right relationships.
In Adam Grant’s research and book, *Give and Take*, he demonstrated that **givers** are the people that contribute to others without seeking anything in return and have the most powerful networks. They move in the world and offer their time to provide advice, share knowledge, or make valuable introductions. **Takers**, on the other hand, are only focused on the “what's-in-it-for-me” mindset. They try to get other people to serve their ends while carefully guarding their own expertise and time. We encourage you to not be a **taker**. Build your network by being a resource to others.

When you find yourself in a difficult situation, an effective approach is to reach out to other experts in your community who can quickly give you real advice that does not have strings such as selling their professional services.

There is also a principle in life that states, *you must first accumulate power before you need it*. This means that nurturing relationships and being a resource to your network comes first. You want to have the network already strong, vibrant, and established before your next major crisis. We cannot stress the importance of continuously engaging in activities that further support your network, a vital aspect of proactivity.

Although proactively building and supporting your network is a good practice in general, it is especially important in security. As a community, we have not been doing as good of a job as our adversaries. Hackers and cybercriminals regularly exchange information with each other and collaborate against common targets and enemies that they have. Sometimes they pay each other as part of their interactions in the cybercriminal underground and as part of a cybercriminal value chain. However, we are pretty sure that no cybercriminal has ever lost a week or two before potentially collaborating waiting for a nondisclosure agreement to be signed. Also, many companies sometimes keep details about who they think may be attacking them close to their vest, instead of sharing

---

3Grant, A. (2014). *Give and take: A revolutionary approach to success*. London: Weidenfeld & Nicolson.
details that could help companies jointly fight against common adversaries. In the past decade, there has been more information sharing across security teams than ever before, with high-tech companies collaborating in confidential, vetted groups and financial institutions also doing so in groups such as FS-ISAC (the Financial Services Information Sharing and Analysis Center). That said, we’re probably still as a community not sharing as aggressively and as fast as cybercriminal groups.

Some specific reasons why you want to have access to a powerful support network include:

- Benchmarking with your peer group. Try to better understand industry trends based on what your colleagues are seeing vs. what your vendors might be leading you to believe. For example, the Building Security In Maturity Model (BSIMM) benchmark allows one to assess the maturity of your organization’s software security practices as compared to peer organizations.

- Threat intelligence sharing groups can provide information about particular adversaries that are targeting the sector that your business operates in. Such groups also exchange technical indicators of compromise (IOCs) and indicators of attack (IOAs) in the form of malicious URLs, hashes/signatures of malware, and other signs that one can automatically scour systems for to determine if an adversary has been targeting or has successfully attacked your systems.

- Contacts within the FBI and DHS provide you with faster access to information on nation-state adversary threats and better engagement. This also means that you find ways to give back to support their ongoing cybersecurity work.
Be a credible source of talent referrals as well as providing references and background information on candidates going through the hiring process.

**Be Prepared**

Andy Grove, the former CEO of Intel, believed that even though you can’t possibly have a formal plan for every possible situation, you still must plan ahead and be prepared:

*You need to plan the way a fire department plans: It cannot anticipate where the next fire will be, so it has to shape an energetic and efficient team that is capable of responding to the unanticipated as well as to any ordinary event.*

Preparation is key, and when applied systematically, it can make all the difference between a limited incident and a large-scale breach that wipes out hundreds of millions of dollars of shareholder value. Times of chaos and intense public scrutiny are not the best time for developing a coherent process and a communications strategy. In other words, be prepared and ready. Do not wait for a call from the FBI informing you that they believe that your systems might have been breached or until a *Wall Street Journal* reporter reaches out to your firm requesting comments on a potential issue before you enact your plan.

**Regularly Evolve Your Incident Response Strategy**

We have urged companies to not treat incidence response simulation as an annual event, as is necessary (but far from sufficient) by various compliance standards. Incident response strategy should be a living process that continuously evolves alongside your organization. Assess your

---

*Grove, A. S. (1983). High Output Management. New York, NY: Souvenir Press.*

203
internal capabilities as well as develop relationships with external incident response service providers and law firms that specialize in cybersecurity to support your internal team. Having reputable firms engaged before you need them might be one of the best decisions you make.

As part of this preparation step, also engage with business stakeholders. For example, over the past several years, we have seen that working closely with your head of marketing or CMO is vital for digital businesses. Every minute of everyday marketing data that has partial and oftentimes complete PII is flowing between your systems and external partners. Developing a good working relationship and understanding between these functions ahead of a real incident is vital.

Engage Forensics Firms Before You Have an Incident

As part of your incident response strategy, you need to ensure there are at least two well-regarded forensics firms engaged with your organization with a retainer and an agreement in place. We say at least two because in the midst of a crisis you want to have redundancy in case one of the firms is already consumed by a similar incident at another customer or might not have the right talent available to you. If you do have a significant breach, you are going to need two firms because you want them to check each other’s work (similar to seeking a second doctor’s opinion). Do not assume that each firm would treat the incident in the same way. If you ever find yourself in a situation where you may have to testify to Congress at some point about a breach, what the firms discover and document and the actions that they help you take in the midst of a breach investigation are of immense, critical importance. It could even make the difference between whether or not you’ll end up in front of Congress for the wrong reasons. Because of the role that forensics plays, you want to have them engaged as early on in the process as possible to aid in containing an attack in progress and with investigation of the breach or security incident after an attack.
Cyber Insurance

Calling an insurance company while the building is burning down to get a quote on fire insurance policy is clearly too late, and the same goes for a cyber insurance policy. A good policy needs to be in place prior to the discovery of a breach. Cyber insurance policies should be chosen and tailored to your business. Determining what your crown jewels are, how much consumer PII you have, where it is stored, and how much coverage you need is a critical first step. A good cyber insurance policy can cover many of the costs associated with a network security incident (IT forensics, legal expenses, data restoration as well as breach notifications to consumers), network business interruptions (lost profits from security failures), and privacy incidents and liability coverage (class action litigation and legal expenses and fines). The broad category of errors and omissions coverage can also potentially be included, and specific riders may also be available for specific types of incidents such as ransomware attacks.

Practice Your Communications Tools and Process

Regularly practice and stay sharp with your communications. Is the list of leaders and executives current? Are you sending sensitive information to a cell phone that belonged to your former CFO? How often do your managers wait before telling HR when an employee or a contractor has been terminated? Once HR has been informed of the termination, how quickly is that information acted upon to cut off access?

One underlying key part of being proactive is to constantly practice the basics and get the basics right. Pilots are required to keep flying and landing their jets, regardless of the number of past missions. Firefighters are required to get dressed and be ready to respond within a set time. Adopting those types of practices is key to being crisp and clear with both your external and internal communications.
Also, the ability to quickly spin up a security war room and get all the key stakeholders engaged to collaborate on working an incident is of critical importance. Running such war rooms is challenging when all employees are on site, at the same location, and looking at the same whiteboard and screens. Running such war rooms is even more challenging when everyone is working remotely and has to coordinate virtually rather than be in one place looking at the same set of screens, whether it be due to an incident occurring on a weekend or due to employees being forced to work from home during COVID-19 shelter-in-place orders.

Be Paranoid

Assume that the attackers are already in your network and have access to some of your systems. The hope is that they have not already compromised critical infrastructure, but ask yourself—if they did, how can you systematically identify them and kick them out? In addition, given the mobile nature of the devices connecting to your corporate systems, assume that part of your network and some of your employees have already been compromised.

Assume that cybercriminals already know some of your employee passwords and can log in to their accounts. Some of your employees may be using the same passwords for their corporate systems as they are for their personal online accounts at popular web mail, social media providers, and file sharing services. As large numbers of stolen credentials from such services that have been breached are available on the dark web, cybercriminals and nation-state attackers try using those to log in to corporate systems. Even if you are using multi-factor authentication, once a password is stolen, employees can be duped and socially engineered to click “Approve” login requests on their mobile devices that are not their own and done with a password bought off the dark web. You can partner with companies that monitor the dark web for a living to determine which
of your employee’s corporate passwords may be in common with those in stolen or purchased online password dumps, and you can have those passwords reset proactively. When you hear of a competitor’s data sold on the dark web, don’t rejoice but double down on your efforts with your team to understand how you could have avoided such an attack yourself or at least reduced its impact on your brand and business.

There are some interesting sayings in the information security field—one is “There are two kinds of organizations. Those that have been breached and those that don’t know that they have been breached.” (See Figure 9-1.)

Paranoia is an important part of the right mindset to achieve security. In general, people that are the most successful in business are confident and optimistic—such is the right mindset needed to grow a business. On the other hand, the right mindset to prevent loss of business is to be paranoid and assume the worst. A middle ground is to have a healthy paranoia that will keep the team sharper than a more complacent team that’s reactively waiting for an alert or a red alarm to go off. The paranoid

---

5www.tag-cyber.com/media/charlie-ciso/only-two-kinds-of-companies
The team is constantly looking for new instrumentation to give them more visibility—both deep and wide coverage. They monitor their networks and the redefined boundaries created by the public cloud and SaaS providers. They are also not just looking down on the technology, but also looking up to see how their business and strategy are changing—and learning what new products or services are being planned that might introduce new vulnerabilities. Finally, the paranoid managers are able to both continue to practice the basics and deliver the fundamentals with excellence while also working with new security startups to learn how innovation can be applied to better protect their organizations.

Habit 2. Be Mission-Centric

This second habit is probably one of the most fundamental and critical habits for any organization that wants to increase its odds of avoiding a severe breach. We begin with a general discussion about management attention. By doing that first, we want to admonish the reader to connect the dots between security and their organization’s mission. Cybersecurity is not just an information technology (IT) issue to be addressed by a small part of the overall organization. Security needs to be evaluated from the lens of how it can help support your organization’s mission—regardless if that means a not-for-profit, a government agency, or a fast-growing business.

Organizational Focus

Leaders across all organizations focus their time, resources, and management attention on furthering the organization’s mission. Ultimately delivering outcomes and keeping their commitments to their stakeholders is what gets rewarded. Issues or priorities that are not considered “critical issues” for the business get less priority, less
discussion, and often fewer resources—capital and human. Trust is usually central to an organization’s mission—whether it be the trust of the customers, users, partners, or employees—and security provides one of the underpinnings upon which trust can be based. As such, we have attempted to share primary learnings from the world’s most impactful breaches, and by now it should not be difficult to have a line of sight between good security practices leading to good business operations.

Mission-Centric Activities

All successful organizations are always engaging in three discrete activities, which we describe here briefly.

Mitigating Risks

Every business has risks—competitive risk, strategic risk, compliance risk, operational risk, financial risk, and, of course, security risk. On the security risk front, each day brings with it new threats that need to be addressed. Mitigating threats that can harm the business and the shareholder’s interests must be dealt with. Risks can be created or can change as a result of many factors: economic downturns, pandemic, regulations, trade conflicts, and technology disruption, to name a few. Such risks can evolve slowly or appear suddenly. When it comes to cybersecurity risk, which may involve risk due to breach, risk due to compliance, and risk due to regulation, such risks can be mitigated in a variety of ways, ranging from employing technology to prevent or detect potential compromise or breach, instituting processes to monitor the risk, or even transferring the risk by getting a cyber insurance policy (ideally after lowering it as much as possible internally).
Fulfilling Obligations

Meeting business obligations and objectives is the second set of activities that must be addressed. Businesses are constantly managing their many obligations to all of their stakeholders: employees, customers, partners, and shareholders, or owners. Paying taxes is an obligation that can quickly become a threat. Adhering to federal employment guidelines is an obligation of any business in the United States. Delivering quality products with the right levels of security and privacy is an obligation to customers.

Taking Advantage of New Opportunities

Creating new opportunities is about advancing the business and moving faster than your competitors. Expanding opportunities ranges from bringing new products and services to market and launching new business models to expanding into new territories. Businesses that do not respond to new opportunities and also create the markets will find themselves less relevant and, over time, will stop growing and eventually die.

Security can also be an enabler for taking advantage of new opportunities. Achieving good security and then taking credit for good security through achieving relevant compliance certifications can often enable a business to grow faster. While your competitors are trying to improve their security posture, you can move in faster and capture more market share. For example, satisfying HIPAA compliance, for instance, can open up sales to medical/healthcare markets. Satisfying SOX security controls enables a company to go public. Satisfying FedRAMP can open up opportunities for contracts with government agencies.

Security as Sales Enablement

In our experience, we have seen large enterprise partnerships get awarded to the business that has been able to demonstrate the highest level of security over their competitor. For example, in the emerging space of
autonomous mobile robots (AMRs), companies that are awarded large contracts are able to demonstrate their robots are secure and hardened in such a way that they cannot be remotely controlled and hijacked to be used as a terrorist weapon in public spaces such as airports. What was once seen as an IT issue to be managed in the technology silo has emerged to be a major enabler to help the sales team. In the era of big breaches, the lowest price offerings might no longer satisfy enterprise customers with major threats and obligations to oversee. Major enterprise deals are closed when the vendor has competitive pricing and a credible security story that can be described and demonstrated.

We will discuss in Chapter 11 the importance of being effective storytellers and weaving a narrative. This responsibility falls on the senior security and technology leaders to help the other business leaders understand how cybersecurity is a critical issue that needs to be considered when evaluating business threats, fulfilling obligations, and exploiting new opportunities to accelerate growth and gain market share. In our roles as CTO and CISO, we have personally made sure that sales and marketing teams are armed with a compelling narrative that demonstrates superior security over the competitors. The larger your customer, the more they may appreciate learning about your security program.

**Pulling It Together**

We have found that one of the effective ways to increase the focus and connect the dots is to contribute to the same strategic plan that is shared with the board and senior executives and demonstrate how the cybersecurity programs support and enable the business to operate and grow more safely. Every day there will be an opportunity to develop and hone this habit. Every day there are new threats that will need to be navigated.
Security Is Risk Mitigation

There are still far too many organizations that have not evolved their approach to managing security as a risk management exercise but treat it as merely another IT “tax” for the geeks to address. Such an approach is both dangerous and shortsighted for the organization as a whole.

Since today’s modern businesses are powered by technology in just about every aspect, security is much broader than an isolated set of technical problems to solve. As you review the following questions, think about whether they are simple IT or security issues that can be dealt with in a silo or if they are connected to the overall mission of your organization and require other major stakeholders in the company:

- Do we enable two-factor authentication on our mobile app to protect privacy or leave it alone to reduce friction and usage?

- How many different passwords do we want employees to maintain to access our internal systems? What will be the impact on employee productivity?

- Marketing wants us to share our data sets with their outside consulting firm—they sent us a secure Dropbox link. We need them to analyze this data quickly to help us launch our new promotional program.

- We need to delay patching our mission-critical systems until our busy peak season is over—we will be roughly six months behind on patching some critical vulnerabilities.

- Our innovation team has built its own Heroku infrastructure outside of our controls. They said not to worry because there is nothing running that is critical yet. But we’re now getting access requests to open connectivity to our production AWS environment.
• We can’t onboard our largest new client this quarter because they had some bad audit findings during their last reporting year. Let’s stall the implementation.

Each day there are many questions and discussions like the ones mentioned above taking place in corporations between employees just trying to get their jobs done and security teams. Expanding the aperture of these discussions to include business leaders to help in defining the best course of action for your organization is vital for avoiding unnecessary trouble down the road. We also recognize that general managers and business leaders might not have the interest or had much background to feel qualified to engage in the broader security topics, but we have found that with some time and learning a few fundamentals, it is possible to offer credible perspectives and help guide the teams to making better risk-based decisions. Peter Drucker wrote, “The focus on contribution turns the executive’s attention away from his own specialty, his own narrow skills, his own department, and toward the performance of the whole.”6 We hope that we have offered a compelling case for why we need each executive to focus on the whole of the business by engaging with the technology and security leaders.

Habit 3. Build Security and Privacy In

_An ounce of prevention is worth a pound of cure._

—Benjamin Franklin (1736)

Security and privacy need to be built into an organization at multiple levels, starting with an organization’s culture, in order for that organization to systematically produce offerings to the market that are secure and

---

6Drucker, P. F. (2011). The essential Drucker selections from the management works. London: Routledge.
protect the consumer’s sensitive information. Having company leadership, including the CEO, CTO, and CISO, present at company meetings regularly to educate employees about how other companies are getting hacked, the right mindset, and providing tips as continual reminders on avoiding social engineering attacks helps create the right culture.

One important part of creating the right culture, after making sure that the right mindset, values, and principles are instilled into the culture, is to create “soft” and “hard” incentives that favor security. As an example of a “soft” incentive through gamification, Salesforce, and specifically innovators who have worked there such as Masha Sedova, developed a company-wide, Star Wars–themed security awareness program in which every employee started off as a “Padawan learner” and could grow to become a Jedi master by not falling for the phishing email, detecting the mole walking around the company without a badge, and generally exhibiting positive security behaviors that would be tracked and used to reward employees. Incentivizing the right behavior through “hard” incentives such as financial bonuses or penalties or incorporating security behaviors into employee performance reviews helps reinforce a culture of security. Alternatively, setting the expectation that software developers should produce secure code and penalizing them if there are security vulnerabilities identified in their code can help create hard incentives. Such hard incentives and expectations may also result in your managers hiring engineers that value shipping secure products, especially if the incentives and penalties “roll up” to impact managers as well.

Beyond creating a company culture supportive of security, a deeper level in which security and privacy need to be built-in is in the area of development of software products. Although no service or application is perfect, approaching security by design means that you have thought through the core architecture of how the service will be implemented and deployed in production. How many points are allocated in each sprint to address the vital nonfunctional requirements that will protect and secure the user’s data?
From looking at a new acquisition target to launching a new partnership, trust should be part of the discussion from the inception to launch. Do not settle for the argument that “security will slow us down... we will bring them in later.” That sentiment should be a signal that business leaders and security and technology leaders need to work better together. Keeping the security team out is no longer a viable solution, and by the board setting the tone, it will become an issue for the management team to address and resolve. Employing the principles of secure design will help produce a far more secure solution than throwing a product over the wall to the security team after the service has been deployed.

One needs to employ a set of well-known principles in order to design security and privacy into a product. Back in 1973, Jerome Saltzer and Michael Schroeder published a paper entitled “The Protection of Information in Computer Systems” in which they described several timeless principles that apply to designing security and privacy in even today. We recount a subset of these principles here with some more modern examples, including some aspects of the breaches discussed in the first part of this book.

Keep It Simple (“Economy of Mechanism,” “Least Common Mechanism”)

Complexity is the enemy of security. The more complex anything is, the harder it is to reason about it. So, the old adage “Kiss: Keep it simple, stupid!” (or KISS) bears weight in security as well. In Saltzer and Schroeder’s original paper, they discuss complexity in terms of feasibility of being able to inspect code line by line and unwanted access paths that

---

7Saltzer, J.H., & Schroeder, M. (1975). The protection of information in computer systems. Proceedings of the IEEE, 63, 1278-1308.
will not be noticed during normal use. However, the point of managing complexity applies at the macro-level as well—to the entire systems and collections of systems. For example, as large companies become even larger through acquisition, it is important to simplify once an acquisition takes place, to avoid having a plethora of potentially redundant, complex legacy systems that perform similar functions. Maintaining each such system and keeping them all secure is considerable work. Some organizations that are good at doing acquisitions ensure that once an acquisition has closed, there is a well-defined integration period, after which many of the redundant systems at the acquired company will be retired. (Or alternatively, the company may decide to choose to standardize on a system from the acquired company that will replace a system from the acquirer, taking the best of what both the acquirer and acquiree have to offer.) In any case, once the integration of the acquisition is complete, there should only be one system responsible for a particular function (accounting, enterprise resource planning, customer relationship management, source code management, etc.). As such, only one such system needs to be maintained, patched, penetration tested, and so on.

Fail-Safe Defaults ("Secure by Default")

Don’t rely on the user to change any setting to be secure. Be paranoid—assume they will almost always get it wrong. The default setting should be the more secure setting. For example, Amazon S3 buckets should be set to private by default. Also, don’t ask the users if they want to make an exception, say, to visit a page that might be infected with malware—they may undoubtedly do so and can get infected.
Create a Security “Choke Point” (“Complete Mediation”)

If there are multiple ways to authenticate into a system, they all need to be checked for correctness, and each of them is a distinct path that an attacker can attempt to find vulnerabilities in and/or bypass. By having a single “choke point” and just one way to do it for a critical function such as authentication, all efforts can be invested into getting that one mechanism right. One might argue that by having one mechanism for authentication, if an attacker bypasses that, they’ve got the keys to the kingdom, but if there are multiple, it gives them more than one option to find something to bypass.

Principle of Least Privilege

The principle of least privilege states that users and programs should only be given the minimum amount of privilege that they need to do the job they are required to and no more. Thinking back to the Apache Struts vulnerability from the Equifax breach in Chapter 4, web servers do not need to run as an administrator to serve web pages. Such access can allow attackers to copy a file with malware into shared memory, make the file executable, and run the malware. Thinking back to the Marriott breach from Chapter 3, a production database with up to 500 million user records ran a non-whitelisted query issued by a human that was not a query used by any of Marriott’s automated systems. Production database privileges could have been configured to only run whitelisted queries used by Marriott’s legitimate automated systems. Thinking back to the Capital One breach from Chapter 2, the S3 bucket with 100 million credit card applications may not have needed to be accessible by the web application firewall.
Open Design/No Security by Obscurity

Assume the rebels will get the Death Star plans. Or, in the world of computer security, assume that the attackers will get your architecture diagrams and your source code. Do not assume that just because things like source code or configuration files are not initially easily accessible, the attackers won’t eventually get them. As such, do not store secrets such as cryptographic keys in them.

Many systems have been hacked because source code or configuration files stored in public repositories such as GitHub had cryptographic keys for APIs, SSH passwords, and database credentials embedded in them. Thinking back to the Equifax breach in Chapter 4, once attackers had initially broken in by leveraging the Apache Struts vulnerability, they would not have been able to access databases internally if database credentials weren’t stored unencrypted in the obscurity of files on disk.

Ease of Use/Psychological Acceptability

If the secure way of doing things is too hard to use, users will inevitably get it wrong or work around the secure way, usually resulting in insecurity. A simple example is that if one increases how complex passwords should be to such a great degree, then employees may begin to use post-it notes on their laptops to remember the passwords. Stronger passwords prevent a remote brute-force attacker from breaking into the system. However, passwords that are too complex cause users to write them down, which weakens the overall security and the intent to harden login credentials. Users should ideally be using password managers (such as 1Password, Dashlane, and LastPass) that allow them to have automatically generated, strong, complex passwords, but that are easy enough to use that they are much more preferable to writing down passwords on post-it notes.
A seminal paper around ease of use and security is Doug Tygar and Alma Whitten’s “Why Johnny Can’t Encrypt.” In that paper, the authors find that PGP (Pretty Good Privacy), a product designed to allow users to securely email each other, was so hard to use that 25% of users in their study actually ended up inadvertently sharing their private/secret keys with people they were trying to communicate with, resulting in compromise of their secret keys.

**Avoid Security Design Flaws**

To complement the preceding security design principles that make up the principles to employ, there are also a set of key design flaws to avoid, as described in “Avoiding the Top 10 Security Design Flaws” published by the IEEE Center for Secure Design. The top 10 security design flaws are discussed in much more detail in the 2014 paper co-authored by Gary McGraw, Neil Daswani, Christoph Kern, Jim DelGrosso, Carl Landwehr, Margo Seltzer, Jacob West, and a host of others in the field. The group that developed these top 10 security design flaws came together from both top high-tech companies (Google, Twitter, HP, RSA, Intel) and top academic institutions (Harvard, University of Washington, George Washington University). The industry participants analyzed data from vulnerabilities in their products and the top design flaws that led to them. As per Gary McGraw’s past work, vulnerabilities were root caused to either be the result of design flaws or implementation vulnerabilities (“bugs”). A **bug** is an implementation-level software problem. Bugs may exist in code but never

---

8Ukrop, Martin & Matyas, Vashek. (2018). Why Johnny the Developer Can’t Work with Public Key Certificates. 10.1007/978-3-319-76953-0_3.

9Arce, I., Clark-Fisher, K., Daswani, N., DelGrosso, J., Dhillon, D., Kern, C., Kohno, T., Landwehr, C., Schoenfield, B.S., Seltzer, M., Spinellis, D., Tarandach, I., & West, J. (2014). Avoiding the Top 10 Software Security Design Flaws.
be executed. A **flaw**, by contrast, is a problem at a deeper design level and may result in multiple implementation vulnerabilities.

The top 10 security design flaws (paraphrased) are:

1) Earn or give, but never assume, trust.
2) Use an authentication mechanism that cannot be bypassed.
3) Authorize after you authenticate.
4) Strictly separate data and control.
5) Define an approach that explicitly validates all input.
6) Use cryptography correctly.
7) Identify sensitive data and how to handle it.
8) Always consider the users.
9) Understand how integrating external components changes the attack surface.
10) Be flexible when considering future changes to objects and actors.

The first design principle is at the heart of zero trust architecture, in which users or devices are not trusted just because they are present on a corporate network. Rather, the assumption is made that users or devices on a network can be compromised and need to authenticate themselves to internal services every time.

The second design principle is the complement of “complete mediation/use a choke point” from Saltzer and Schroeder’s security design principles. Even decades later after the initial publication of those security design principles, data from top high-tech companies were analyzed, and it was found that many security vulnerabilities originated because complete mediation was not being employed.
We refer the reader to the original “Top 10 Security Design Flaws” paper for a detailed description of the other eight design flaws, but do feel it was important to at least introduce both the principles to “do” and the don’ts—the flaws to avoid—that make up the habit of designing security and privacy in.

Habit 4. Focus on Security First; Achieve Compliance as a Side Effect

*Management is doing things right; leadership is doing the right things.*

—Peter Drucker

When we consult with companies and boards, we try to quickly assess what kind of security program is being presented to us or discussed. We become concerned when the focus of the discussion is about compliance frameworks and audit results. We listen for what is left out. What about the real world, in-the-trenches security countermeasure and controls, and tactics that are required to safeguard the organization? We begin to wonder what kind of problems are hiding underneath the compliance activities and the checkboxes being checked. Drucker’s famous quote that management is doing things right while leadership is doing the right things applies to this habit. We believe that following a strict compliance program without the right security tactics and controls is like doing a lot of things right; that approach will certainly earn you some points and help you pass compliance audits. However, the resources and focus going into compliance might not be the right things for your business or appropriate for protecting your most valuable data and assets. Hence, it might not be addressing the most important things—the right things for your organization.
Defend Your Turf Like a Security Rebel!

A helpful analogy here is America’s revolutionary war between the British Redcoats and the new American renegades fighting for independence from the king of England. The British Army followed specific protocols of what defined legitimate and orderly warfare: they stood in a single line and row formations—it would have been dishonorable to not follow centuries-old traditions in how they marched to battle, stood on the frontlines, and faced their enemies—in this case, the natives and American rebels. The Revolutionaries had employed different tactics against the more organized army and well-supplied British Army. They fought a different war and deployed new tactics: guerrilla warfare. They hid and surrounded their enemies, attacking from the rear, and they dressed in civilian clothing, and even sometimes in disguise. They were able to successfully push back the all-powerful British forces because they were innovative with their tactics.

What we are advocating for here is to embrace cybersecurity as American Revolutionaries and deploy tactics that are effective for your given threats and risks in your business. Abandon outdated “traditions” or activities that no longer serve your business but were part of “this is how we do things around here.” Avoid doing things that either take attention away from the core issues or, worse, give you a false sense of security by having long compliance checklists that do little to actually protect your business and customers from the real threats. Thinking like a hacker is a far better posture than thinking like a classically trained IT auditor.

Examples of a defensive technology that take such an approach are “deception” technologies and honeypots. Such technologies create a plethora of seemingly real but virtual systems and targets for adversaries to attack. If done correctly, attackers will not be able to distinguish between real and virtual systems, and it will give them so many potential internal targets to attack that it may just be easier for the attacker to
pursue targeting another organization. No compliance standard (at least today) requires the use of deception technology, but leveraging deception technology is a great way to defend your turf like a security rebel!

Applying this approach requires that cross-functional teams are formed to look at the business holistically and think like a hacker who is hell-bent on breaking into the environment. It means that the security team has to be deeply embedded into the corporate IT and product development teams and truly understand the end-to-end deployment architecture. It requires the courage to make the right calls. For example, prioritize securing the back-end ecommerce platform and front-end to the ecommerce system and deprioritize patching the in-room iPads that power the conference room technology and calendar.

We are not trying to discourage the reader from adopting and applying compliance frameworks so long as the primary purpose is to advance the security program. Too many times, organizations get so consumed by complicated regulations and audits that they stop focusing on real security altogether. They point to the latest checklist as the validation that they are well protected. Our plea is that focus on threat detection, predictive controls, preventive controls, and detective controls will provide high-quality defenses which lets compliance be a byproduct of good security practice rather than the other way around.

Habit 5. Measure Security

Famous management consultant Peter Drucker once said, “If you can’t measure it, you can’t improve it” (*The Essential Drucker*). So is the case with security as well. In this section, we discuss the importance of both quantitative (as well as qualitative) measurement and how measurement can be used to achieve a level of security well beyond that can be achieved by simple compliance with security standards. Checking a compliance checkbox—either you have a security countermeasure in place or you don’t—is typically not sufficient to achieve security. The real question is
how good the countermeasure is. Having some countermeasures in place to check a box could potentially be better than having nothing, or it could provide nothing but a false sense of security if the countermeasure is not effective.

W. Edwards Deming is similarly credited with saying “you can’t manage what you can’t measure.”¹⁰ Note that just because you can measure and manage something, that doesn’t mean it is important or the right thing to measure. That said, once you have determined what the right thing to do is, you can figure out what is the right thing (or set of things) to measure and then improve against it.

We provide examples of how to measure security quantitatively (and qualitatively) as well as what is worthwhile and not as worthwhile to measure from the areas of anti-phishing, anti-malware, and software vulnerability management, three of the six technical root causes of security breaches.

**Measuring Phishing Susceptibility**

Given that phishing is a prevalent root cause of breaches, one can have employees take anti-phishing social awareness training in which they are sensitized toward telltale signs of phishing attacks to make them less susceptible to falling for attacks. Many compliance programs require security awareness training, but just having employees take the training to “check the box” does not tell you how effective the training is.

Many information security teams send out fake, test phishing campaigns to gauge how effective such training actually is based on the anti-phishing part of security awareness training. The hope is that employees will be less susceptible to falling for phishing attacks after the training as compared to before the training and how much less susceptible

---

¹⁰Kaplan, R. S., & Norton, D. P. (n.d.). The balanced scorecard: Translating strategy into action. Boston, MA: Harvard Business School Press.
can be quantitatively measured. There are challenges, of course, as each
test phishing email is different, and it may be hard to establish if employee
phishing susceptibility is actually lower or higher due to how deceptive or
tricky any given phishing email is. That said, over time, and with enough
tests, one can quantitatively measure if there is a trend in employees
becoming less susceptible to phishing attacks.

Measuring employee susceptibility to phishing, though, may not
be worthwhile to do if an organization has more or less eliminated the
threat of phishing attacks by deploying hardware tokens required for
authentication, such as YubiKey. That said, phishing emails could still have
malicious links in them, even if their credentials can’t be phished. Without
having strong anti-malware defenses in place, an employee device could
still be infected even if their credentials cannot be stolen or abused with
multi-factor authentication in place.

There are also other employee behaviors to measure around
phishing—if part of the advice to employees is to report potential phishing
attacks to the information security team, one can also measure the
percentage of employees who report test phishing emails to the security
team. Even better, when employees report real phishing attacks to the
information security team as a result of appropriate training, the number
of such phishing attacks getting reported can be quantitatively measured.

In addition to quantitative measures, it may also be a good idea to
do some qualitative measurements. In one organization that one of the
co-authors has worked in, after deploying security awareness training,
employees would start forwarding phishing emails to the information
security team, proud that they didn’t fall for the company’s phishing tests.
Some such emails turned out to be real phishing attacks that employees
thought were test phishing attacks sent out by the information security
team! Although it may be impossible to quantitatively measure what
percentage of real phishing emails are being reported to the security team
(as the denominator, the number of real phishing emails that are being
sent to employees, may be unknown), it is a very good qualitative sign when employees are trained to be aware enough that they start reporting real attacks into the security team.

**Measuring Malware Detection**

In another example from the area of malware protection, your company may be running an anti-virus protection suite. Check. Compliance achieved. But how good is the protection offered? Some anti-virus protection suites are free, while others cost money, and there is an old adage: “You get what you pay for.” That said, just because you pay a lot doesn’t necessarily mean you get the value for which you are paying.

Anti-virus protection can be quantitatively tested based on how much known malware they detect, and that is easy for testing organizations to measure. You simply take a large catalog, potentially of hundreds of thousands of known malware samples, and run them through the anti-virus engine. An anti-virus engine with up-to-date signatures may detect 100% of known malware samples. But is that what matters? Is the detection of known viruses the right thing to measure?

Rather, what really matters is what percentage of **unknown** malware is detected by the anti-virus package, not based on known signatures, but based on more sophisticated algorithms (e.g., artificial intelligence/machine learning). Cybercriminals and nation-states will typically develop new malware variants and run them through all anti-virus packages or at least the anti-virus package being used at a particular organization that they are targeting. Once they arrive at a variant that accomplishes their attack of interest that is **not** detected by the anti-virus package(s), only then do they release it. Hence, what is important to quantitatively measure is: what percentage of previously unknown malware is the anti-virus package able to detect? Detection of previously unknown malware samples is what matters, and that is what is important to measure quantitatively.
Another example from the area of software vulnerability management might be patching third-party software vulnerabilities within some number of days as required by an internal security policy, as required by, say, the PCI compliance standard.

An example of such a vulnerability is CVE-2017-5638, the Apache Struts vulnerability that was used in the Equifax breach that allowed attackers to remotely issue commands of their choice without authentication. One might be, indeed, patching 100% of such vulnerabilities within the required period and complying with the standard. Many organizations are hard-pressed to simply achieve that compliance. However, even if one is achieving that goal, one might ask if that is the right goal to achieve.

Some vulnerabilities may or may not be exploitable, even if they are critical vulnerabilities. CVE-2017-5638 was an example of a vulnerability that was easily exploitable. That said, if the Apache Struts server in the Equifax breach was protected by a web application firewall (WAF), that may have prevented the vulnerability from being exploitable.

For a CISO, whose job may be on the line based on such vulnerabilities that could be exploited, it may be important to have security and IT teams first focus on vulnerabilities that are exploitable. There are so many new vulnerabilities getting discovered that teams typically have to prioritize which vulnerabilities to resolve first with their limited resources, as resolving vulnerabilities takes work. As such, if a vulnerability cannot be exploited, resolving it should have a lower priority as compared to a vulnerability that is immediately exploitable.

That said, the number of immediately exploitable vulnerabilities that can be taken advantage of may also be more than some security and IT teams can handle at any given time. In addition, some vulnerabilities may or may not be getting exploited in the wild. That is, while it may be possible to theoretically exploit a vulnerability, attackers may or may not actually
be exploiting it in the wild for a variety of reasons. As such, having threat intelligence as to which vulnerabilities are actually being exploited in the wild can be very valuable in prioritizing which vulnerabilities to resolve first.

So instead of considering all vulnerabilities together and just measuring whether or not they get resolved in a given compliance period, it may be more worthwhile to measure, say, the average amount of time that it takes to remediate critical, exploitable vulnerabilities. The faster that an organization gets at resolving critical, exploitable vulnerabilities, the more actually secure it will be against real attackers, as opposed to just being able to exhibit its ability to comply with standards. It is important not only to get all the vulnerabilities resolved but to get the most critical ones that could actually be used to breach an organization resolved fastest.

**Habit 6. Automate Everything**

As of the writing of this book, the information security field is heavily understaffed, and chances are that it will continue to be for some time. Even with appropriate staffing, though, human capacity cannot scale to meet security challenges in large environments, whereas automated prevention, detection, and containment can. As such, the sixth habit encourages practitioners to automate as much as possible.

Similar to the concept of secure defaults, it is highly advantageous to have secure behavior and processes automatically happen. There are typically too many processes in enterprise systems to manage, and every time that a human has to remember to do something for security, the more likely it is that the right thing could get forgotten or delayed, which can give an attacker the window that they need to compromise or breach a system. As such, anytime that security can be automated, the better.

For example, relying on end users to manually patch software is a recipe for disaster. Most end users will ignore repeated requests to patch their machines, as their focus is on being productive and getting their work
done. Dialog boxes reminding them to patch are interruptions that are easy to ignore and get in the way of their jobs. Information security teams that have to also send out continual reminders to patch can be viewed as nags, and there are much better uses of attention and “airtime” that security teams can engage with employees on. As such, using software that automatically patches itself is a much more reliable approach to making sure that critical vulnerabilities in software get patched in a timely fashion. Some software packages, such as the Google Chrome and Mozilla Firefox browsers, automatically patch themselves regularly. If only all software could auto-update as such! So, when possible, give the users an opportunity to cancel the update once or twice (to avoid an interruption during an important sales presentation), but at some point, the patching process should be forced along with a reboot.

Automatic scanning and patching can also be applied to servers. In order to have a scalable security and IT program that may have purview of hundreds of thousands or millions of servers, automated configuration checking for security appliances and many other devices must be a part of an organization’s security posture, and we cannot rely on humans for such things. For instance, in the cloud, tools such as Dome9 and Evident.io can be used to automatically scan for such misconfigurations, and it would be great if tools could ideally fix them too. The Capital One breach was one example where a firewall misconfiguration in a hybrid cloud/on-premise environment resulted in a significant breach that could potentially have been avoided if there was automated scanning and remediation. Environments such as those at Capital One are way too large to be able to rely on IT or security administrators to always be expected to get things right and manually review thousands or more firewall rules.

Of course, one should also put some automated checking and monitoring in place to notify a human if automated security process is not running, as automation can break or the automation itself can be attacked. How do you make sure that the automated checker is also checked? There are many technical solutions to that including using watchdog processes,
in which two automated processes regularly check that each other are functioning. If one of them fails, the other restarts the one that failed. Only in the case that both automated processes crash at the same time does the automation break, and watchdog processes are more resilient to a single automated process failure.

**Habit 7. Embrace Continuous Improvement**

In the book *Atomic Habits*, James Clear writes about the British Cycling team in his introduction. Clear describes how habits, small or even insignificant, have a *compounding effect* over time and why making small improvements on a daily basis can lead to a significant difference in the long run. He then goes on to tell the story of Dave Brailsford, the British Cycling coach. Brailsford brought a new approach to the team—the philosophy of *continuous improvement*. The primary concept was the principle of “marginal gains”:

> *The whole principle came from the idea that if you broke down everything you could think of that goes into riding a bike, and then improved it by 1%, you will get a significant increase when you put them all together.*

The British Cycling team adapted the habit of continuous improvement and went on to win multiple Tour de France as well as Olympic gold medals multiple times over several years. As we conclude this chapter on the habits of effective security organizations, we want to encourage you to leverage the power of “1% Better Every Day” as you adopt these habits to your organization and continue to build and improve upon them. The magical aspect of this approach is that just about any organization can improve in small, *atomic* increments and get far in one or two years. We agree with Clear’s thesis: “Success is the product of daily habits—not once-in-a-lifetime transformations.” This thinking
has significant implications for organizations and not just the personal domain. It is the difference between setting one large project as the goal and embracing a continuous improvement habit that accepts many small wins along the way.

Once you can quantitatively manage various aspects of your security posture, continuously work to improve them as nothing is ever 100% secure. Constantly improve your countermeasures, and measure improvements quantitatively whenever possible.

Summary

In this chapter, we have presented the seven habits of highly effective security. We have distilled our combined 45+ years of technology and security experience into the foundational habits that when practiced daily will help you achieve positive security and business outcomes. The seven habits for highly effective security are:

1. Be proactive, prepared, and paranoid.
2. Be mission-centric.
3. Build security and privacy in.
4. Focus on security first; achieve compliance as a side effect.
5. Measure security.
6. Automate everything.
7. Embrace continuous improvement.

Proactivity, preparation, paranoia, and continuous improvement (Habits 1 and 7) can produce effective security programs just as they can produce effective people. People focused on security should be mission-centric first, focusing on the larger needs of the organization and how
security supports the larger goals of the organization (Habit 2). Effective security is built into an organization and into a product—it is not an afterthought (Habit 3). Saltzer and Schroeder’s timeless principles can help one practice Habit 3 to achieve security.

Security should be the goal, and compliance with security standards should ideally be accomplished as a side effect of achieving the goal of security (Habit 4). Compliance should be viewed as a minimum bar and is not sufficient to achieve security. If the minimum bar is used as the goal, and that goal is even slightly missed, insecurity is likely to result in addition to noncompliance.

Security can and should be measured both quantitatively and qualitatively (Habit 5). In particular, the effectiveness of countermeasures that help prevent the root causes of breach are wonderful things to measure quantitatively to set an organization on a path to quarter by quarter lower its actual probability of breach.

Good security processes should be automated by machines, and not left to error-prone humans (Habit 6). Security processes that are automated and that humans don’t have to think about create a secure-by-default environment. Techniques from the world of fault tolerance can help ensure that automation failures are much, much less likely than human failures.

Finally, with quantitative and qualitative measurements in place, continuous improvement should always be practiced as nothing is ever 100% secure.