CHAPTER 1

Information Security: Adventures in Culture Hacking

You don't have to go digging through technology news feeds for evidence that the world of information security is in a state of crisis. Data breaches are all over the mainstream media. Enormous in scale and frightening in their implications, major security incidents seem to be happening with alarming regularity. When it is not shady criminal hackers perpetrating the theft, we worry that it might be a hostile government gearing up for a new kind of warfare, or even our own government embracing a new age of Orwellian surveillance possibilities. And the message that resonates from the pages of information security industry magazines and websites to the keynote speeches of industry conferences and the marketing brochures of product and services vendors is, *InfoSec is broken somehow—it doesn't seem to work anymore.*

Maybe. Society has undergone profound changes with the widespread adoption of digital, networked information technologies. Some theorists speculate that these changes are structural, representing not just new features of traditional society, but new definitions of society itself. In this view, we are going through changes like those that happened when human beings stopped being nomadic and established agriculture and villages, or like the transformations that took place during the Enlightenment, or as a result of the Industrial Revolution.

Such evolution means that everyone, including the information security industry, better be ready for changes unlike anything we've previously experienced. Technology has become social, centered around people, and information security must become equally people-centric if it hopes to succeed. We not only have to do things better, but we have to invent whole new ways of doing them. That means looking at things that have traditionally made security experts, especially technologists and engineers, uncomfortable. Things that are hard to measure or automate. Things like people, including their beliefs and assumptions as much as their behavior. Things like culture.

Burnt Bacon

I first realized the power of culture in information security a few years ago at a supplier conference hosted by a customer. Dozens of reps from different vendors filled a large hotel ballroom reserved by our host. After we had all grabbed our coffees and sat down, the executive running the event called the meeting to order with a safety briefing. He introduced us to our safety officer, let's call him Bob, who also worked for the customer. Bob was not an executive or even a manager. But before turning over the microphone to Bob, the executive made it clear that, in terms of our physical safety and security, for the next two days Bob might as well be the CEO.

I had not expected the briefing, but I wasn't very surprised. The company running the conference operated in several hazardous industries and prided itself on the "culture of safety" it instilled in employees. Bob spent about five minutes running us through a review of safety protocols for the event, pointing out all the exits, telling us which we should use in the event of an emergency, and even declaring a rallying point across the street. Should something happen that required us to leave the building, everyone was required to meet at the rallying point for a headcount prior to returning or taking whatever other actions Bob deemed appropriate. Once he had finished, Bob took his post at the back of the ballroom and the day's activities commenced.

I *was* surprised when we returned from the first day's lunch break and the executive again handed Bob the mike so that he could repeat the same briefing we had listened to only four hours before. "Wow," I thought. "These people take safety seriously." I had never experienced that kind of briefing before at any of my own company's meetings, much less two in the same day at the same event!

Coincidence is a funny thing. Just over an hour after our post-lunch briefing, the hotel fire alarm began to wail. On reflex, everyone turned around to look at Bob, who immediately slipped out of the room. Within a minute, the alarm stopped. A minute or two later Bob returned with one of the hotel managers in tow, who was obviously trying to explain something. I watched Bob shake his head "no," prompting the manager to leave. Ten minutes later, I was standing with my fellow vendor representatives across the street as Bob took a head count.

We found out later that the manager had contacted Bob to tell him the fire alarm had been triggered by a small grease fire in the kitchen, but that it had been contained and posed no danger to our meeting. Bob had not bought the explanation and had triggered an evacuation anyway. We were the only ones to leave the hotel after the alarm, and we caught more than a few curious glances from people passing by. Once Bob was satisfied everyone was present and that the hotel was not actually on fire, he gave the all clear and we filed back into our seats in the ballroom. Despite the minor nature of the fire and the fact that unnecessarily evacuating had cost us nearly an hour of our packed schedule, the executive never gave a hint of annoyance. Instead, he called us back to order by spending another few minutes praising Bob's decision and reminding us that, for his company, safety came before anything else.

The second morning of the conference consisted of breakout sessions scattered in smaller rooms throughout the hotel conference center, but they began only after our morning safety briefing was complete. We broke again for lunch, and when we returned to the ballroom in the afternoon, the executive was waiting for us. He was not happy. Standing in front of the room, he held up one of the vendor packets each of us had received at the start. Stamped "Highly Confidential" on every page, the packets were the blueprints of the company's forward-looking IT strategy, including strategic competitive differentiators enabled by technology adoption.

Waving the packet slowly so that we all could see it, the executive chewed us out, describing how the document he held had been discovered in one of the empty breakout rooms during lunch, left there by someone in the room. He explained with obvious irritation that such blatant disregard for protecting sensitive corporate data was unacceptable, especially in a room that included many information security professionals. If it happened again, he warned us, there would be hell to pay. And with that, we started up again, beginning once again with our mandatory safety briefing.

Safe and Not Secure

An important characteristic of culture is that it tends to be invisible, functioning just below our conscious awareness of its influence. But that often changes when we find our own cultural norms challenged, and suddenly we see patterns and conflicts jumping out at us from the shadows. Take, for example, the stark contrast between my customer's *safety* culture, where the response to the possibility of an incident brought all business to a stop and triggered emergency action plans, and the customer's *security* culture, where an actual security incident resulted in nothing more than a stern talking-to. The two completely divergent responses to essentially the same thing, a failure incident, made the differences between the safety and security cultures of my customer stand out from one another like black and white. "Wow," I thought, "one of these things is not like the other." It was astounding.

My customer believed they had a strong culture of safety. They also believed they had a strong information security culture. But culture is defined by behaviors, not beliefs. The completely different behaviors they exhibited between the two incidents showed where their priorities really lay. Had the executive treated the failure to secure sensitive information like Bob had treated a burnt rasher of bacon, we would have stopped the proceedings immediately until he resolved the problem. Instead of ordering an evacuation, he would have ordered everyone in the room to hold up their vendor packets. The documents were controlled, and at least one person would not have had one.

What Were You Thinking?

I found myself obsessing over the experience for the rest of the day. It distracted me from focusing on the presentations and the interactive sessions. I was distant and disengaged. Why had the executive just let that security incident slide so easily? He had been visibly angry over it, but he could have done much more than scold us. Was he worried about embarrassing people? Had the evacuation thrown us so far off schedule that he was just trying to make up for lost time and not delay the event further? Thinking that maybe he intended to follow up later and try to track down the perpetrator some other way, I checked for unique identifiers on my packet that could have tracked it back to me directly. I found nothing of the sort.

For a little while, I got depressed. I had traveled a long way to attend a meeting that was all about how important security was to this company, only to watch a senior executive get upstaged by a junior employee when it came to taking action in the face of risk. The response to the security incident called into question the whole purpose of the conference. If the company wasn't going to take action when faced with a security breach involving one of their own information security vendors, how were they ever going to protect themselves from the real bad guys? It would all be technology products and lip service. They didn't care enough to make a real change. I found myself thinking, "They should put Bob in charge of information security."

Then I realized something else. I considered the real, physical harm that I knew this company had seen as a result of lapses in workplace safety. People had been injured on the job, had even died, in the decades that the firm had been working in the industry. I knew the firm had also experienced information security breaches in the past, but my impression was that these failures had rarely risen above the level of a moderate inconvenience. People had a bad day, to be sure, but at the end of it everyone went home safely. If the information security culture was not as strong as the safety culture, it was because the world of information security just didn't *feel* as dangerous as the world of workplace safety. No matter what they said, this company could not think about data security the same way they thought about physical safety. Those cultures could exist side by side, but the assumptions and beliefs that drive behavior, born of experience and observation, were just not the same. I was fascinated and, once more able to focus on the customer, made a mental promise to research the topic further.

So here we are.

Culture Hacking

This book is about culture. It is about understanding it and about transforming it. You can even say it's about hacking it. And when I say *hacking*, I mean hacking in an old-school sense, the hacking that Steven Levy described in *Hackers: Heroes of the Computer Revolution*. Before the term evolved (some might say devolved) into today's more familiar usage, with all its implied negativity and criminal inferences, hacking described a process of gaining knowledge about a system by exploring and deconstructing it. This knowledge would then be put to use to make that system better, more innovative and elegant. The MIT hackers that Levy wrote about dealt in computer software, the programs and digital code that define how those systems function. But systems, code, and hacking don't stop there.

Software of the Mind

Researchers and experts in organizational culture talk about their topic in ways that would not be completely unfamiliar to computer engineers. There are many frameworks and metaphors for describing organizational culture, but all converge on the idea that culture is a shared set of norms, values, and routines that serves to define how people behave together in organized group settings. If you have ever started a new job, then you have probably experienced a cultural shift as you had to learn how things were done at your new organization, and maybe some of those things were completely foreign to you. But as you learned the ropes, as the culture was transmitted to you and you became part of it, things that you had to think about became automatic and unconscious behaviors. It's almost like the organization programmed you to function within it.

Geert Hofstede, one of the more influential scholars in the field, talks about organizational culture in just this way. For Hofstede, culture is "software of the mind" that allows individuals to align their thoughts, beliefs, and actions in order to solve specific problems. Nowhere does Hofstede, or any other culture researchers I am familiar with, claim that people are programmable in the same way computers are. But these experts do look at organizations as complex systems that share similarities with computers and networks.

By using metaphors drawn from software and computing, we can conceptualize and identify means of understanding how culture can be observed, measured, and changed. Thinking about organizational culture as a different kind of software, with its own codes and programming techniques, makes the hacking analogy a lot more applicable. In fact, the security industry already uses the analogy all the time when talking about social engineering. The idea of hacking people is not new or even very controversial in our industry. But social engineering has always focused primarily on individuals, treating each potential victim as an independent system that must be exploited. You can automate social engineering, as does an attacker who conducts mass phishing attempts by using automated group e-mail tools, but this only allows the attacker to target individuals more quickly and efficiently. It's simply a question of scale.

Hacking culture is different from hacking computers. It means understanding and exploring the relationships between people, the drives and motivations that cause many unique individuals to behave in very similar ways, as a group. Instead of trying to affect the behavior of individual people making specific decisions, a culture hacker is more interested in understanding and changing the entire group's behavior, by changing what that group thinks and believes. Part of hacking is about elegance and efficiency, the ability to produce the greatest effect with the least effort. If you focus on my individual behaviors, trying to change them one at a time, you will be lost in an infinity of inputs and outputs. But if you are able to understand and change my beliefs and assumptions, you will have tapped into the programming that drives all my decisions.

Hacking a person's belief systems may seem kind of creepy, and culture hacking can certainly be put to evil uses. But hacking has never just been about breaking into computer systems illegally or immorally for illicit gain. That's a narrow definition that has, unfortunately, come to be the most associated meaning of the word, thanks to the media and, ironically enough, the security industry. But hacking is much more than that, with a longer history than the one information security has tried to impose on it. Culture hacking is similar. I didn't invent the concept, and it's been around for a long time. I just believe it's a very useful way to think about the challenge of people-centric security.

A Brief History of Culture Hacking

The first people to call themselves culture hackers came from the worlds of activism, fashion, and art. They wanted to shape the way the world looked at itself, to shake up the status quo, and to pull the curtains back on people's preconceived notions. For Mike Myatt, a leadership expert and author, hacking in organizations involves breaking down existing codes and complexity, finding alternatives, and replacing out-of-date or inefficient processes. That's old-school hacking.

Culture hacking is pre-digital, going back to practices like billboard jamming, literally changing the messages on real-world roadside billboards from advertisements to more ironic or anti-corporate messages. These techniques date back to the 1970s, developing in parallel with phone phreaking and the beginning of computer hacking. It wasn't about stealing or defacing private property; it was about retaking control of the system from those who had corrupted it, to make it free again. This was the '70s, remember.

Though it started out fueled by flower power, culture hacking has proven remarkably resilient. As the world changed, so did the focus of the movement. Culture hacking and technology merged with the creation of groups like the

Adbusters Media Foundation, which both uses and critiques digital technologies. In 2011, Adbusters was central in creating the Occupy Wall Street movement. Throughout its history, the mission of culture hackers was to reshape behavior by targeting basic social programming, usually with an anti-authoritarian and anti-corporate bias, just like many of the early computer hackers.

Whether or not you grok the whole anti-establishment theme, hacking (computers or cultures) is a set of techniques and tools for exploring and deconstructing complex systems for the express purpose of changing them, making them work differently, evolving them. Depending on what side of the fence you are on, this can be a process of innovation or a process of manipulation and abuse. But then again, you can say that of just about any tool. A hammer can easily become a nasty weapon.

Security Culture: Hack or Be Hacked

I believe that culture is the single most important untapped resource for improving information security today. Security is not a technology challenge. If it were, technology would have fixed the problems a long time ago. Security is a people challenge, a social and organizational challenge. It's a cultural challenge.

People, and how to deal with them, seem to especially baffle information security professionals, to the point where we have trouble even talking about the human beings that make up our organizations as anything other than problems to be dealt with, insider threats to be identified and managed, or risks to be mitigated, preferably by automating them away. When we do think about people, we tend to think of them as targets for attack or accidents waiting to happen. Steeped as the industry is in a background of engineering and applied technology, we can be deeply ambivalent about the qualitative, the emotional, or the political—in other words, all the things that make up the organizational cultures in which information security has to operate. Given the industry's mistrust of people in general, it's not very surprising that the idea of people-centric security has taken a while to gain traction.

The industry is changing, becoming more cognizant of the importance of people to the successful protection of information assets and information supply chains throughout the global digital economy. We're not changing because we have suddenly seen the light and developed a new appreciation for the chaotic and irrational human networks we must secure. We're changing, at least in part, because we've tried everything else, it's still not working, and we're desperate. And that's okay. Sitting in my vendor conference, I had the epiphany that my hosts didn't take information security seriously because they had never experienced any really serious problems related to it, certainly not like they had with physical accidents and losses. I was sure that as soon as they did experience a catastrophic information security event, they would attack the problem with the same commitment and zeal that had created their impressively formidable safety culture. Today's information security environment is changing dramatically. Today you either hack your own culture or you wait for someone to do it for (or to) you.

Who's Hacking Your Security Culture?

Think for a moment about the culture hackers in your own security program. They may not be immediately apparent. Your first thought might be the security awareness team, if your organization has one. These brave souls are presently the tip of the spear when it comes to security culture transformation, although we will see in later chapters that the challenge they face is often impossibly idealistic. But if you are looking for those folks beating the behavioral drum and trying to change the way the entire company thinks about security, awareness teams are top of mind.

Security awareness managers are probably not the only ones socially engineering your organization's security beliefs and practices. Think about your auditors, for example. Audits, particularly those for regulatory or industry standards like the Payment Card Industry Data Security Standard (PCI DSS) or Sarbanes-Oxley, have a material effect on a company's ability to do business. Internal audit and compliance teams are responsible for making sure the company doesn't fail audits, and they do their best to transmit and instill certain beliefs and rituals into the larger enterprise. A strong audit culture is unlikely to believe, for instance, that documented processes are unnecessary or that every employee should have complete access to every system in order to stay agile. Given the importance of maintaining compliance, auditors also typically have the power to reprogram the organization's focus and activities, even if only temporarily.

Finally, think about the project manager or line manager who has no direct responsibility for security but can reward or punish his employees based on their job performance, through promotions and pay raises, or even by firing poor performers. Every organization has priorities, and these do not always align. In fact, they can compete directly, a situation we often see in information security as a sort of Rubik's Cube effect, in which improving one part of the problem makes another part worse.

Imagine our project manager running a software development team working on a new product. Bringing the project in on time and on budget is a major priority for the company. So, too, is ensuring that the product does not have security vulnerabilities. What happens when there is not enough time to do both? For example, suppose a developer realizes she has seven days to finish her work before deadline but that a full security review will take ten days. She could go to her manager and tell him that she will complete the review, because security is a priority, but that the project will be late to market. Her manager's response will be key. Whether he gives her praise, like Bob received when he put safety first and evacuated over a minor incident, or punishes her with the loss of a bonus or maybe even her job for delaying the project, he will show everyone what the company values most. When that choice comes up again, everyone will know what to do.

Now imagine that you are the security awareness manager for this example firm, or another member of the security team. If the cultural bias is toward deadlines, how can your values compete? Security awareness suddenly becomes more complex than just making sure all the developers know the policies on secure coding and testing. Our developer was already aware of her responsibility for security. But if management rewards and punishes based on project deadlines, or budgets, or some other factor, no amount of handwringing, training sessions, or posters on the wall will change a developer's empirical understanding that security comes second. That's cultural engineering.

Security, Hack Thyself

You don't have to have a graduate degree in organizational psychology to become a culture hacker, any more than you need one in computer science to become a technology hacker. What you do need is a new way of looking at your organizational environment and the people in it, which requires imagination and a willingness to experiment. Technology hackers don't let others tell them what the system can or cannot do, but instead figure it out for themselves by exploring the system. If you want to hack culture, you have to learn how the culture really works, not just what everyone thinks or expects of it.

The closest this book gets to a manifesto—and a first principle that anyone seeking to transform their security culture must become comfortable with—concerns the role of people in information security. In a people-centric security program, human beings matter every bit as much as technology, and probably quite a bit more. Technology enables people, not the other way around. Technology neither cares nor suffers if it is hacked or compromised, at least not yet. If you were to throw every IT asset your company owns out the window tonight, tomorrow morning when everyone shows up for work you would still have an organization.

Kick out all the people, on the other hand, and tomorrow you will have a warehouse full of stuff with no one left to care about whether or not it's secure.

Computer systems are immensely complicated, designed and built from hardware and software, governed by extraordinarily intricate architectures and millions of lines of programmatic code. For all that, computers have finite limits to their capabilities. People define what computers can do, and they do only what they have been programmed to do, even in situations where those possibilities are not what the programmers expected or intended. There are always clear reasons for a computer's behavior, at least once you have tracked down those reasons to root causes. But complexity is different. Complex systems produce emergent behaviors, an infinite possibility of outcomes that is impossible to predict. Those behaviors may not be consistent, or even rational. People and social systems are complex in ways that a computer can never be just on its own. But plugging a computer into a social system like a company or a government creates new avenues for complexity and emergent behavior. People-centric security recognizes that focusing on technology systems alone will always be a losing battle because technology-centric security is invariably outflanked by emergent human behavior. The moment you think you're covering all the angles, someone will figure out how to square a circle and produce four more new angles where none previously existed.

Hacking your security culture, as opposed to hacking your IT infrastructure, means digging into the forces that motivate people's security-related behaviors within your organization. You have to analyze not only what your systems do, but what people are doing with them, how they are adapting them to new and innovative purposes. Some of these new uses will create risk, but also opportunity. Culture defines the interface between users and systems. If you want to transform your organization's security culture, to make it better and more efficient at protecting organizational assets, you have to pull apart the people system as well as the process and technology systems, so that you know all of them inside and out. It isn't enough to just observe what people do, or do with the technology at their disposal. You have to understand why they do it, and try to consider all the possible alternative decisions they could have made, rather than just the one that may seem obvious or expected.

In the years since I sat in that hotel conference room and realized the differences between a culture of safety and a culture of security, I have observed dozens of other organizations' InfoSec cultures. Every one has had something to teach me. Even when I cannot get a customer to think about culture as much as I might like, they always manage to keep me thinking about it. And I can tell you that culture hacking in the security space is a zesty enterprise, regardless of whether the organization is even aware they are doing it.

Culture Hacks: The Good

It's always great to work with an organization that takes culture seriously, without discounting it as too vague or paying lip service to its importance but never really trying to change it. I've even encountered a few organizations that embraced the cultural transformation of information security full on, with all the messiness and uncertainty that come with that sort of work. In the case of one particular organization, I had come in to help them define a new enterprise security framework, a governance program that would tie together all the disparate and sometimes dysfunctional silos and pockets of security ownership that had grown up organically over the life of the company. As we walked through the various options for designing the new program, the security team kept trying to articulate what they really were trying to achieve. They had needs and requirements that spanned people, processes, and technology, and our conversations often got specific and detailed on one or more desired outcomes, but nothing ever seemed to completely hit the mark. "Yes," they would say, "we need that. But we need much more."

The organization was intrigued by ISO 27001, the international standard for security program management, and asked me a lot of questions about what I thought of it. I told them I thought very highly of ISO 27001. When properly and conscientiously implemented, ISO 27001 can function as a very powerful governance framework, one that I also think happens to be the most people-centric security standard out there today. I told my customer so.

"But ISO isn't for everyone," I cautioned. "It's not about technology or even controls. The standard is about changing what your whole organization thinks and believes when it comes to information security. Implementing ISO to me is about driving a process of cultural transformation in regard to security across the entire enterprise."

The team members' eyes lit up. Eureka! That was exactly what they had been struggling to articulate. They didn't just want a new security program, they wanted a whole new security culture. "We don't want to just change the mechanics," they explained, "or to switch out one set of controls or one best practices framework for another. We want to change what security means to the company, and we want to change it for every single person who works here regardless of rank or role." Amen, I thought.

That's a good culture hack, or at least the beginning of one. The security team wanted to change behavior, but recognized that behavior grew out of something deeper. That was where they wanted to concentrate their efforts. It helped that the company was already a self-consciously strong culture. The idea of social identity and shared beliefs permeated its business. The security team already had a template and a language that were familiar to them. Believing in the power of culture in general makes it a lot easier to see the benefits of improving security culture in particular.

Culture Hacks: The Bad

Not every organization thinks in terms of transforming their information security program or culture. Some security teams are so swamped just keeping on top of operational activities and deadlines that thinking about why they do things the way they do, or whether they could do them better, seems like a luxury. It's hard to think about a five-year improvement plan when the auditors are coming next week. In fact, compliance drives so much security activity today that it's probably the main motivation companies have for taking security as seriously as they do. ISO 27001 is a voluntary security standard, but most companies are dealing with the nonvoluntary sort. PCI DSS for credit card processors, Sarbanes-Oxley internal control requirements for publicly traded companies, HIPAA regulations in healthcare, along with a slew of other local, national, and transnational regulatory regimes may put constant demands on the attention of the Chief Information Security Officer (CISO).

Security compliance efforts are a bit of an attempt at culture hacking themselves. Regulators and industry groups develop compliance requirements as a means of forcing organizations to take security more seriously. This is great insofar as it improves the final product. But when compliance replaces security as the goal, cultural transformation backfires. It's like the old Zen warning not to mistake the finger pointing at the moon for the moon itself. Compliance is not the same thing as security, as has been made painfully clear by recent security incidents where auditors had previously signed off on the very systems that ended up being compromised.

I've observed more than one organization where the security culture has been trained and conditioned by compliance programs to equate successful audits with good security. Even when certain folks inside the organization know better—and often these are the security operations people, who know how the sausage is made, so to speak—the shared assumption is that if the auditors are happy, the organization must be secure. That, too, is a form of cultural transformation, just not a good one.

Culture hacks are bad when they make the system easier but don't actually solve the problem. Knowledge of the system is partial or incomplete, making a culture hacker feel like they have accomplished something more than they actually have. To extend the metaphor, those who put total faith in a one-size-fits-all compliance checklist are like cultural script kiddies, interested more in quick results than in deep and lasting change.

Culture Hacks: The Ugly

Even when the efforts at cultural change are unsophisticated or incomplete, the people trying to change things usually have good intentions. Most security teams are passionate about what they do and are deeply concerned with making their systems safer and stronger. But there will always be outliers, individuals and organizations whose security behaviors are so egregious that you almost have to think they want to fail.

I visited an organization once where the security management team members were some of the most arrogant jerks I had ever met. Even though I had been hired to help them, they belittled and second-guessed everything I or my team said. When we asked if they had a particular control or process, they would roll their eyes. "Of course we have that," was the answer. "That's security 101. Is that all you smart consultants can ask us?"

In the organization's defense, it did have a formidable set of controls in place. A lot of highly sensitive data passed through its systems, and the information security team made it difficult within those systems to share the data without jumping through administrative hoops. "We lock our people down tight," senior leaders bragged to us. "No one gets up to any funny business."

When we moved on from the leadership and started interviewing employees who were lower on the organizational chart, we asked about the intense levels of control the organization had put in place. Many of our interview subjects grinned at the questions, then told us stories of how much of a pain it was to share information efficiently.

"Those senior guys you talked to," one employee told us, "all have personal webmail accounts they've set up. When they want to share things quickly, they just bypass the controls and attach stuff to their personal e-mails and share it."

We were shocked. "But they said you guys couldn't do anything like that," we protested.

"Oh, sure. We can't. They don't trust us, and they think everyone who is not a manager is an idiot. But it's not a problem for them. That's just the way things work around here."

Security Is People!

This book is about giving organizations and the people responsible for securing them a new set of concepts and techniques. I'm not trying to replace technology or process as effective tools that are needed in information security. But I am trying to give people, the often neglected third leg of the people-process-technology triad, their proper place. People-centric security means looking at the human element of data protection as more than just another threat vector. People-centric security implies that without people there is no security, nor any need for it. Process and technology are there to support people, both from a security perspective and for the entire organization. Nobody starts out with security but no information to protect. Security needs are born when an organization's information supply chain starts producing valuable assets that demand protection. People define when that occurs, people make protection happen, and people are responsible when security fails.

Culture acts as a powerful engine of organizational security, and in subsequent chapters I'll go into lots of detail about what culture is and how it drives human behavior. But the core premise of everything that will follow is this: if you want to really change how security works, you have to change the culture operating beneath it. Just because security has struggled with the human equation in the past doesn't mean it must continue to baffle us in the future. In fact, it can't. Our world is social, and our technologies are increasingly social. Our security must be social too, retirement puns notwithstanding. People-centric, then. Security is people!

Further Reading

- Adbusters: Journal of the Mental Environment. Available at www.adbusters.org.
- Hofstede, Geert, Gert Jan Hofstede, and Michael Minkov. *Cultures and Organizations: Software of the Mind.* 3rd ed. New York: McGraw-Hill, 2010.
- Levy, Steven. *Hackers: Heroes of the Computer Revolution.* 25th Anniversary Edition. Sebastopol, CA: O'Reilly, 2010.
- Myatt, Michael. *Hacking Leadership: The 11 Gaps Every Business Needs to Close and the Secrets to Closing Them Quickly.* Hoboken, NJ: Wiley, 2013.