Chapter 8
Information Security: Beyond the Bits and Bytes

Mary Ann Davidson

Information security is many things, but boring is definitely not one of them. It's a rollercoaster where the ride gets more dramatic every year, zipping down a plunging chute and taking your breath away. I've worked in information security for most of my professional career. I got into it when I became bored with building accounting software, and there was an opening in a group at my company that was building a product to "automagically" handle data of different security classifications (e.g., people who can only access "Unclassified" information wouldn't be able to view or change information labeled "Secret"). As a former U.S. Navy officer, I knew something about the value of limiting data access based on security classifications. I took a job as a product manager in that team and almost immediately found what "tripped my trigger" in the tech sector: security! Since that first security job, I've worked with a bunch of different teams and technologies and enjoyed (almost) every minute of it.

Working in information security is different from many other aspects of technology in that there are larger issues than the bits and bytes. For example, if you are stranded in the middle of Upper Slobbovia, a map application that knows *exactly* where you are might help you find the fastest route home, even taking traffic and weather conditions into account. Neat, huh? Of course, it is not so neat if someone is able to use those same geolocation services to track your every movement, unbeknownst to you. The same technology that can be used to make lives easier and more productive may also have "unintended consequences." Information security involves actively looking for those "unintended consequences." As I learned from military history, "where there is capability, an enemy may develop intent."

M.A. Davidson (✉)

D.A. Christofferson (ed.), *Women in Security*, Women in Engineering and
Science, https://doi.org/10.1007/978-3-319-57795-1_8

Security Is a Team Sport

You only as good as the people willing to work with you and for you. That is, the old security saw about “a chain is only as strong as its weakest link” is even truer when it comes to building a strong security team. You want really good people with a variety of skills and—equally important—a variety of *viewpoints.* Unless you believe you are like Mary Poppins— “practically perfect in every way”—it’s really important to have people working for you (and with you) who have a diversity of viewpoints and the freedom to express them. You will make better decisions that way: I know I do.

My team encompasses people with a variety of skills. Ethical hackers try to break our products and services before bad guys do; vulnerability handlers help developers find, triage and fix security vulnerabilities; program managers implement the assurance program by which we “build in” security across the breadth of our products and service offerings; security evaluators certify our products against relevant U.S. and international security standards (such as the U.S. Federal Information Processing Standards (FIPS) 140, to validate our encryption implementations). We work also with other security experts across the company in a variety of areas: legal, public policy, compliance and operational security. My job in information security is many things, but it is never boring.

Soft Skills Matter

Even if you are a technical whiz like the ethical hackers who work for me, you still need to hone other skills, which can be equally important in your ability to be an effective information security professional. One if the more important skills is—communication. Yes, I know, not a “sexy” skill, but still very important. For example, the real job of ethical hackers on my team isn’t “finding security problems,” it is explaining *what* they found, *how* they found it, in a way that the larger lessons are captured and mere mortals can understand and act upon the information. If you start a discussion with “here is how we trashed your code,” the people who wrote the code will get very defensive and not listen to you. If you start with, “we are here to help you by finding problems, explaining them, and giving you a chance to address them,” you will get more “takers.” De-geeking the speak is important, too. If you say “there is a clearly a BBSP in the frabistat object leading to a CST,” you might as well be speaking Homeric Greek: you won’t be very well understood. (Admittedly, I made up those acronyms.)

Two of the soft skills that have worked well for me are the ability to use analogies and to analyze problems in economic terms. Analogies are important because they help people understand something by relating an unknown to something they know: “this is like that.” I create analogies when someone is explaining a technical problem to me, to help ensure I’ve understood the problem correctly. Sometimes I use an analogy to illustrate a larger truth. For example, there is a huge gap between the industry need for cybersecurity experts and the number of people who can fill those slots. "We need more cybersecurity experts!" is a true statement but it ignores what I think is the bigger problem.

Remember the story of the little Dutch boy, who, detecting a leak in the dike that surrounded his town, bravely put his fingers in the hole to prevent a flood. Too many people think the answer to cybersecurity threats is more little Dutch boys—tens of thousands of them—to plug all those holes! The real problem is a failure of engineering, the result of which is that sooner or later, all those dikes will break and we will have 30,000 drowned Dutch boys. In short, we need to engineer our systems to be more secure and more attack resistant, or we will never be able to hire enough "Dutch boy cyber defenders" to secure them.

Economics rules the world, because there are some fundamental truths that affect what you do and how you do it, no matter what business you are in. One of them is that resources—time, money and qualified people—are always limited. Sure, you may be able to hire more people—if you can find them—but you likely will never have enough time, money *and* people to do absolutely everything you want, all at the same time, to perfection. That is all the more reason to look at what we do from the perspective of what matters the most, and what we can do that is highly *leverageable*. My team has embedded security requirements and checklists into the tools development organizations already use to track milestones (better to fill out one checklist than two checklists—it's faster and easier). We use metrics to enable development teams to manage their own workload better ("here are the most important things to do first"), which helps teams use their resources better. Cost avoidance is another economic way of thinking about security, especially, the business case for finding and fixing security issues earlier. It's better to fix something earlier, once, than have to fix it later—and more expensively—across X supported versions and Y operating systems. Economics is your friend, especially when it comes to "doing the most security good in the most efficient way."

Change Is a Constant

Mechanical door locks haven't changed all that much in eons. There are tumblers, there's a key: the fundamental mechanisms are pretty well understood. Most of what we deal with in the information security world isn't so static. (Not even what we call it: we've morphed from "computer security" to "information security" to "cybersecurity.") Information security changes rapidly because information *technology* is changing rapidly. There are some fundamental security truths (rule 1 is "never trust any unverified input" and rule 2 is "see rule 1"). However, the technology changes, where we use it changes, and how we interact with it changes, even if the threats just get exploited in new venues and new protocols. In short, you need to be adaptable if you want to work in information security.

My team has adapted what we do to the increased delivery of information technology as cloud services rather than on-premises products. The move to cloud in no way diminishes the importance of security and provides new opportunities to have better security at lower cost. For example, when you deliver a product, you don't always know exactly how customers will use it in their systems. You should—and most vendors do—deliver a secure default configuration so a customer is reasonably secure "out of the box," but you can't know everything about all customers' security needs. Similarly, when you drive a new car off the lot, the seatbelts are already configured and the air bags are ready to deploy, but the manufacturer cannot know how much leg room the driver needs, so the driver must adjust the seat to her liking.

With cloud offerings, if you are the one running them, you have a much better idea exactly how they are going to be used, which makes it easier to lock them down ahead of delivery, increasing security "out-of-the-box," and at a lower lifecycle cost. Even better, you can do things that lead to lower cost of secure operations (like having specific audit options on by default): stronger, repeatable, "operationalized" security. I enjoy watching technology change and ensuring that what my team does continually adapts and improves security.

Embracing change also means that you reexamine your beliefs and your practices from time to time. Business changes, customer expectations change, threats change, and that means that you need to ask questions like, "we've been handling Y a particular way and for what were good reasons at the time we created our policy. Is that still the right thing to do?" Never say never, and be willing to reexamine what you do and why you are doing it.

Integrity Is key

Integrity in the information security context means that data has not been altered inappropriately: that is, you have confidence that "A" is "A" and not "B" that has been futzed with—inappropriately altered or corrupted. That kind of integrity is really important because data you cannot trust is probably worse than no data at all.

There is another kind of integrity that is even more crucial in information security: doing the right thing, including giving your best professional opinion. In security, you may frequently be explaining risks or potential threats to people who are not as geeky as you and, to be fair, have different and perhaps broader responsibilities. Integrity includes giving one's best professional opinion regardless of the circumstances, rather than "telling Ms. X or Mr. Y what you think she or he wants to hear." Of course, part of being a professional is not just describing a problem but providing context (what is the ramification of this?) and ideally a recommendation as to how to address the problem you raised. It also means that, having given your best professional opinion, you implement whatever management decides to do to the very best of your ability.

One of the best parts of my job is that I feel I have always been supported for giving my best professional opinion—even better, I have been *valued* for that. On occasion, a manager may have made a different business decision than I recommended, but the difference has never been one of principle, just a different (yet still ethical) choice. Ultimately, your work environment is perhaps the key factor to success in information security, because you can only effect needed change if you have the ability and the opportunity to “let your ‘yes’ be ‘yes’ and your ‘no’ be ‘no.’” When you work in an area as challenging as information security, with a great team, and your core integrity is valued and respected, it’s a terrific place to be.