CHAPTER

1

The Value of Knowing What NOT to Do

> Experience is knowing what not to do and knowing when not to do it.
>
> —Dennis Coates

Experience is the best teacher anyone will ever have. Pain is one of the best educators any person has ever met. Think about it for a second. Remember the first time you touched something hot? It probably only took once for you to learn, "If the pan is hot; I should not touch it." Odds are, if you're like me, you were a smart-ass kid who looked your parents directly in the face as they told you, "Don't touch that; it's hot." And what did you and I do? We reached out with smug smiles and grabbed that hot pan. And immediately, the lesson became exponentially evident: We should listen. In the half-second it took for the electric signal to travel from our fingertips up our arm, across our chest,

up through our neck, and into our tiny childish brains, we were made aware of the truth that our parents weren't lying to us and that the pan was indeed hot. We were learning in real time that we should not do things that would cause us harm, and we were being educated to trust that those older and more experienced than us were warning us for a very good reason.

Unfortunately for me, I am hardheaded. Although I learned from the hot-pan problem the first time, it would take a potentially life-threatening event for me to learn that I should not ignore the cautions of those who know what they are doing and have the life experience to justify their cautions.

I'm from Texas. I grew up on a farm. Well, a ranch. The nearest town has a whopping population of fewer than 400 people, and I graduated high school with a massive class of 51 students other than myself. In our school, everyone played all the sports, and everyone had to be engaged in every after-school activity simply because there weren't enough people to fill a bus to attend any events. For the district to pay for the gas for us to have an educational program after school, everyone participated whether we liked it or not. It was a town with only three streets and no stoplights. The firefighters operated out of a barn, and in the fall, you were allowed to bring your shotgun to school to go dove hunting in the afternoons. It was as Texas as it comes.

I still love to go home and be with my family on the farm, and I honestly think that's one of the places where I learned some of my most valuable lessons about what not to do and when to listen to people who know what the hell is going on. When you live on a ranch, ultimately, you will have to work the cattle. What does this mean for all you city slickers? Well, it means eventually, you're going to take the herd, no matter how large it is, and get it into a corral and begin to give the cattle all the medications, vaccinations, and treatments they need to stay healthy. The money generated from the sale of those animals feeds your family, and you have

no choice but to make sure they are as healthy as possible so they can get to market.

A rite of passage for most Texas boys is finally getting to work the herd with their father. And just like every other kid in my small town, I couldn't wait for the day I got to work the herd with dad. You had to be physically large enough to be helpful, so you couldn't work the cows until you got to be at least 10 or 11. Luckily, I was a big kid. The first time I did this, I was about 11 years old, and I was tall enough that dad was ready to have me help him work the herd. In Texas, you do this in the spring when the weather goes from cool in the morning to boiling hot in the afternoon. You get sunburned, the air smells like shit and burnt leather, and the experience is genuinely unpleasant. Working the herd is nothing like the romantic scenes you've seen in movies like *Lonesome Dove* or the TV show *Yellowstone*. But it's something that every Texas boy who has access to a ranch and animals wants to do.

The first time I went to the annual roundup, cowboy hat in hand, ready to help dad and other ranchers work on the cows and prepare the herd for the next year, I was excited. I was unafraid, and I was ready to show them that I was a young man and could help do these things, just like the rest of the cowboys. Like every other time before when I had watched from afar, things seemed normal. The herd was driven into the corral, the animals were lined up, and we got ready to begin with the yearlings (cows between one and two years old) at the front of the line for processing. Some cows get big fast and can easily be north of 350 pounds in their first year, but the yearlings are "manageable" as they are smaller.

While these animals look like big, slow, lumbering oafs, they are not. When you take a few thousand pounds of beef and throw it into a corral, and the herd gets the idea that something is going wrong—they can hear the moans and bellows of their fellow

cows as they are being treated, injected, and stuck with a variety of sharp metal objects—their stress levels go through the roof. The yearlings are exceptionally prone to this stress and will do anything to find a way to get out of that corral as fast as possible. (Keep this in mind.) My job as the low man on the totem pole but also the largest kid in the corral was to help push the yearlings up through the corral into a narrow channel or chute that would ultimately bring them in front of the real cowboys who would treat each yearling as it emerged. Sounds simple enough, right?

On my first go-round, I got behind a group of a few yearlings, started whooping and hollering like all the other cowboys, and watched as the herd began to move up into the chute. All was well. "This work is alright; I could do this all day long," I thought to myself. And then the situation began to change. Fast. About the third yearling in line figured out that things were not going to go well for it when it got to the end of the chute. The yearling decided unexpectedly to do a complete 180 and come back out at full speed, directly toward me. If you've never been in a position where a mass of beef is running at you as fast as possible and you have nowhere to go, it's a terrifying experience. Being a young man and typically doing things like reacting rather than thinking, I did what any self-preserving human would do and jumped toward the nearest fence as 500 pounds of beef rocketed past me.

It was probably one of the fastest moves I have ever made in this life, but that quick move resulted in removing the only barrier between the rest of the yearlings and their freedom. In seconds, they discovered they could backtrack out of that chute, and they rushed me in a wave of hoofs and muscle that my young mind could barely comprehend. Before I could turn around to face the chute again, the yearlings knocked me over, trampled me, and kicked me in the face as they vaulted out of the chute. As I've said, I have a hard head, and nothing other than my pride got

seriously hurt. But now I had to push the same animals back into this chute.

The problem was that while cows are simple, they aren't stupid, and now they were aware that they had the power and ability to backtrack out of that uncomfortable place at will. Effectively, the beef was now in charge of the situation and process. So, for the next 8 or 10 hours, one by one, I had to grab a yearling, physically shove it into the chute, and then hold it in position until the cowboys were ready to process it. Our herd at that time was a few hundred cows, which also meant there were a few hundred yearlings, so my friend Gary Lee and I spent the entirety of that day and the next two days getting our asses kicked, stomped on, and shat on simply because I had not stood my ground with the first yearlings I faced.

Where does knowing what not to do come into this conversation? Why am I telling you a story about some redneck kid doing rancher stuff in a book about leadership? Before this engagement, we had a cowboy named Sidney who had been doing cowboy things his entire life. He had the craggy hands, leather skin, and scraggly beard of a man who had spent a lifetime doing hard, physical work. Sidney could easily have been an extra on *Yellowstone*. In the days before we began to move the herd into the corral, Sidney tried to advise me never to back up, knowing that I would be the low man on the totem pole who would push the yearlings into the chute. With a cigarette hanging out of his mouth and a bullwhip in his hand, already three beers deep on the morning before that day in the corral, he looked me dead in the face and said, "Never back up, because if you do, they're going to know they can lick you. They'll figure it out quick, boy. And you're going to spend the rest of your time doing these one by one. And you will get your ass stomped."

I acknowledged Sidney's words smugly, but I did not heed them. I smiled at him and tipped my hat like any good cowboy

would do, but his words passed through my ears like a Taco Bell burrito moving through a freshman's colon. Someone who had the experience and knew the issues I was about to face had told me what not to do: "Do not give those animals an inch. Do not back up. Above all, keep the yearlings with their heads facing forward, and keep pressure on them so they won't move anywhere but where we want them to go." Had I done those things, I would not have spent three days straight moving animals one by one into and out of the chute in the blazing Texas heat.

But what does that lesson have to do with business and knowing what not to do? The lesson I learned that day (aside from how corral dirt tastes) was that even though someone might not be the boss (Sidney was a hand, not the corral boss), those seasoned in the work know what they are talking about and should be listened to. The people who have done and are doing the work have the insight and knowledge that is only learned by failing at something repeatedly. I learned right there, with my face down in the dust and cow crap, that lessons from the people who have been in the trenches have immense value.

In my interactions and workshops with executives, I have seen that this insight is usually woefully absent. I have been in rooms with the highly paid, highly educated executive staff and watched them ignore the advice and lessons of those who weren't present or, worse, were in the room and were blatantly ignored because the muckety-mucks were "solving bigger problems." Okay, maybe they are. Maybe they are thinking on a different plane, but the odds are that they still should perk their ears up. The people who have the scars from doing the actual job know what works and what doesn't.

I am sure that this sounds like "duh" to you. You would think so, but I have found that all of us, especially those in senior leadership positions, spend most of our time with our heads in the clouds trying to solve the "big problems." I have been in rooms

where the person who does the work and has the scars to prove it chimes in on an issue, and although the people in the room don't overtly discount their input (that would be rude), they don't give the person the credit they are due.

You may not get the big idea or the game-changer concept from the people who do the work and make things happen. But at all costs, don't ignore their input. They know what not to do. They have cut their teeth on that misery biscuit and can guide your organization's thinking about what pitfalls you are facing. It's a lesson I learned as a young man after getting my ass stomped for days on end, but I only had to learn it once. Take your time, and listen to those further down the corporate food chain. They may not be the boss, just as Sidney was not, but they can save you considerable pain.

So don't ignore the folks who do the work, especially the older or more seasoned people who know where the bodies are buried. But what about a different example of a senior leader realizing things at the corporate and macroeconomic levels? Are there any examples of a corporate legend observing that everything was wrong and failure was imminent and then making a dramatic change by realizing what not to do? Yup. But I doubt you would think that Steve Jobs is one of the greatest examples of exactly this approach.

If you read books on technology, sooner or later you'll see references to Steve Jobs. It's rare to read anything in technology about products, innovation, or changing the world and not encounter a mention of Steve Jobs. The man rightly deserves all the credit he's been given, as he did essentially change the world. Hell, I have multiple Apple products in my home right now. I use my Apple Watch at the gym. All my photos are stored in my iCloud, and my iPhone is the digital leash that I am constantly tethered to, but that technology also provides me immense value. Steve Jobs was an intelligent businessman and innovator whose

focus on the customer and the product was not seen in the market before he did it. But he was an asshole. And not just a regular one; he was a jerk of epic proportions. His leadership style was such that when employees saw him coming down the hall at his own company, they would find a way to turn and go in a different direction so they did not run into him. Steve Jobs had a small, close-knit group of people who would willingly interact with him even though his wrath was always just a few breaths away. Later in this book, we'll talk about the issues around being a jerk and why that's another no-no for any business leader, but I felt it was appropriate to state for once that Steve Jobs was an asshole. Another life goal achieved.

What can we learn from Steve Jobs that can tell us what not to do? Jobs once said, "Deciding what not to do is as important as deciding what to do." Never were words like that more valid than when Steve Jobs came back to take over Apple Computer in 1997. When he was brought back to help revamp the company, Jobs quickly realized that there were over a dozen different product lines all simultaneously competing in the market. After less than a month of being back on the job, Jobs saw that the way Apple Computer was going about its current business meant it was facing calamity.

Steve Jobs was forced out of Apple Computer in 1985. When it happened, his departure was not much more than a blip on most business radars. He did what promising innovators and entrepreneurs do: left that company and went on with another venture. Although tales of his ousting are the stuff of legend and have a kind of Shakespearean narrative to them, when he was let go, Jobs was noted to have raged at the board with a fury that "scared the shit out of everyone," according to an executive who was present at that uncomfortable meeting.

Following his abrupt departure, Apple Computer's new leadership began to focus on creating technology by combining the

Macintosh computer, the LaserWriter desktop printer, and Aldus PageMaker (later part of Adobe Systems) into a stream of capabilities that would be offered to the market in the mid-1980s. These efforts were all put in motion with the additional objective of Apple Computer maintaining at least 55 percent of the overall market share. And for a while, Apple Computer ran the market. Its numbers and growth were aligned with expectations, and all was well in the Apple Computer kingdom. But that level of production and development combined with compounding capabilities inevitably leads to product sprawl and the increase in price that tracks along with it. IBM PC computers and compatibles introduced essentially the same functionality at an exceptionally lower price, which effectively gutted Apple Computer's position and dominance in the market.

While this combat was taking place between Apple Computer and IBM PC computers, Steve Jobs founded and ran NeXT, Inc. Jobs founded this company to focus on powerful technology that could run enterprise-level applications but was still affordable enough that a college student could purchase one of the machines and use it in their dorm room. While that was a great idea, the overall price of a NeXT computer was more than $10,000, and most college kids didn't have enough money for Taco Bell, much less $10,000 for a nifty box-size computer. NeXT sold only about 50,000 of these machines, most to large government organizations that could afford such a hefty price tag for a sexy, cool workstation. The real innovation NeXT was offering was the operating system, which would introduce the concept of object-oriented programming into the personal computing space. That object-oriented programming innovation ultimately led to the Mac OS X operating system, the game changer in the computer space, when Apple Computer acquired Steve Jobs' company and ported its operating system over.

Once Jobs came back into the Apple Computer family, it did not take long for him to change the company's approach. In less than a month of being back on campus, Jobs realized that there was too much going on for successful execution. Apple Computer was trying to compete at an unachievable price point with technology that was excessively complicated and overpriced for a market that only needed some of the things it sold. The story goes that in one of his many fits of rage, Jobs stood up during a product meeting and drew a square carved into quadrants on a whiteboard. At the top of the quadrant, He wrote "consumer and professional," and on the other axis of the quadrant, he wrote "desktop and portable." Then he turned to everyone in the room and said, "Anything not in those quadrants is canceled." With that simple statement, Steve Jobs effectively canceled 70 percent of Apple Computer's current product line. After a period of stunned silence, the people in the room filtered out, tiptoeing away from the space so as not to incur Jobs' wrath further, went back to their respective work centers, and delivered the news.

Not long after that, Steve Jobs realized that Apple Computer corporate was facing another problem that was undercutting the company's ability to execute and grow. He analyzed the corporate earnings and P&L statements and uncovered a concerning fact. Essentially, he realized that the way the company was accounting for P&L statements among the organizations within Apple Computer needed to be revised. Obliterated was more like it. Because of the fragmented and overly bureaucratic approach, every business unit at Apple Computer had its own individual P&L statement.

Originally, profit and loss were calculated within Apple Computer by each business unit. That accounting and performance strategy was a siloed and micro-focused approach, leading to infighting among the divisions as each tried to determine where to allocate its costs. Managers were only concerned with their units

showing a profit, which meant they were in truth ignoring the company's overall health. They could not see the forest for the trees. Jobs realized this was a critical flaw and only hampered growth and cooperation; he decided, "We won't do this anymore." To fix this problem and remove the primary failure point, he upended the company's management structure. Jobs eliminated every manager at Apple Computer, blew up the complicated business operations, and moved the company away from a practice that made sense for the IRS but not for Apple Computer. His move away from that failure also aided Apple Computer in moving to a model of only one P&L statement for the company, which ultimately improved the company's position and optimized reporting for the accounting group.

Adopting that changed functional structure was innovative for a company like Apple Computer. But thanks to the "We aren't doing business this way anymore" focus of Steve Jobs, Apple still operates this way, even though it is now nearly 40 times as large in revenue and quintupled in headcount. Senior vice presidents oversee the specific functions of the teams, not the output of the products. Steve Jobs died in 2011, but the new CEO, Tim Cook, still occupies the only position on the organizational chart where the design, engineering, operations, marketing, and sales of any of Apple's main products converge. Other than the CEO, the company operates without conventional general managers. No people control the entire process, from product development through sales, and no work centers are judged according to a P&L statement.

So, what's the takeaway from this story? Why do we need another rundown of something unique that Steve Jobs did? You might be thinking, "I thought this was going to be a book about how not to do things." Exactly. By knowing what not to do, such as keeping 40 different product lines all running at the same time, none of which were delivered to customers in a manner

that benefited them, Steve Jobs realized that he needed to draw a line in the sand to say "We're not doing this anymore." By coming back into the company and helping the leadership understand that what they were doing was drowning the company, Steve Jobs ultimately optimized the corporate approach. He changed the accounting practices for one of the most profitable companies on the planet.

Had he not done so, Apple Computer would have continued along its path and ultimately missed becoming a dominant force in computing. The desktop computer space would have passed it. Had he not realized that there were things the company should not be engaging in and that there were only a few exceptionally viable routes to the market, nothing would have changed. There would be no iPhone. There would be no Apple Watch. There would be no iCloud. If ever there was a great example of someone in a leadership position stepping up and realizing what not to do, this is it.

A great example in the cybersecurity market of knowing what not to do and ignoring those warnings comes from observations around the company formerly known as Norse Corp. Norse Corp is one of the most significant examples of how everything that could have gone right for a company went wrong as soon as Norse Corp's kimono was rolled open. How did a company that had the money, marketing, and technology (or so it seemed) not heed the warnings in the fishbowl market of cybersecurity that all of us have heard repeatedly: "Never lie about your technology in a space filled with hackers whose sole purpose in life has been to find flaws and weaknesses in systems"?

In 2012, Norse Corp was known as a cybersecurity industry darling, racking up massive investment, exponential growth, and new clients at an almost unachievable pace. Norse Corp was doing so well that it had the money to hire actors in Viking costumes to show up at various cybersecurity conferences. The real

sexy factor for Norse Corp's technology was its attack map graph, which was quickly adopted by various organizations as their view into the cyber underground. This map was produced in real time and could show a variety of attacks globally targeting infrastructure. It was a well-crafted, sexy map that drew the eye of anyone who happened to come across it. However, that was about as deep as the technology went for Norse Corp.

For four years, Norse Corp was trucking along, doing what all startups want to do: gaining customers and growing. Norse Corp accumulated tens of millions of dollars of funding, which at the time was an excessive amount of investment for a small startup in cybersecurity. Norse Corp was also one of the most active threat-intelligence reporting groups and was deeply engaged with various media outlets. When Sony was hacked in 2014, Norse Corp was the first organization to be on the news talking about the link to a malicious insider. A source of information known only to Norse Corp corroborated the reporting. Norse Corp also published research specifically citing cyberattacks against critical infrastructure that Norse Corp had attributed to Iran. Again, the company's analysis and data were the only sources for that unique insight. Somewhere, alarm bells began to ring, even as Norse Corp grew in the market and continued producing various intelligence reports. But much like Icarus, Norse Corp was getting too close to the sun.

In 2014, Norse Corp was throwing amazing parties at a variety of top Internet security conferences and luring dozens of security experts to come work for the company. One was Mary Landesman, a former senior security researcher at Cisco Systems. Landesman was brought to Norse Corp to be its chief data scientist, and she was so certain about the company's success that she even recruited her son to work at Norse Corp. As the lead data scientist, Landesmann's job was to discover valuable and interesting patterns in the "real-time attack data and cyber threat

intelligence telemetry" that Norse Corp was famous for. However, it wasn't until seven months after she was hired as Norse Corp's chief data scientist that Landesman was provided access to the data that it was part of her job to analyze. To put it bluntly, she was disappointed in the quality and integrity of the data she finally received. She noted that the information she was provided was little more than anyone might glean from an exposed, public-facing web server that was misconfigured. She was quoted as saying, "The data isn't great, and it's pretty much the same thing as if you looked for web server logs that had automated crawlers and scanning tools hitting it constantly." Adding to this failure, Landesman noted that the way Norse Corp collected its data was a protected secret, and only the top three people in the company were provided access to those data streams.

When Norse Corp published its analysis of the industrial control system attacks and attributed those attacks to Iran, the analysis was called into suspicion. Rob Lee, considered one of the greatest minds in the space around industrial cybersecurity controls, gutted the entirety of the Norse Corp analysis on the Iranian critical infrastructure hacks, calling it disingenuous at best and potentially inflammatory at worst. In Rob's counteranalysis, he was quoted as saying, "The systems in question are fake, and the data obtained cannot be accurately used for attribution. In essence, Norse identified scans from Iranian Internet locations against fake systems and announced them as attacks launched by the Iranian government."

In 2016, Norse Corp's CEO was asked to step down by the board of directors. In a rather abrupt series of events, the company went from live and thriving to offline over three days. It turned out that the majority of Norse Corp analysis was bullshit. Its unique insights and detailed analysis of data streams that only Norse Corp could acquire were nothing more than recalibrated, slightly modified narratives that Norse Corp employees

crafted to meet the growing demand from investors and the media. In various critical analyses from deeply educated technical experts in the cybersecurity space, Norse Corp's assertions were eviscerated. Rob Lee is also the co-founder of security software maker Dragos Security, now a billion-dollar cyber unicorn, and a former cyberwarfare operations officer for the U.S. Air Force. He posted a blog stating that Norse Corp was "not a bellwether of the threat intel industry. While their product and Internet level scanning data was interesting and potentially very valuable for research it was not threat intelligence. So while they may have billed themselves as significant players in the threat intelligence community, they were never really accepted by the community, or participating in it, by most leading analysts and companies."

Brian Krebs, a well-known reporter in cybersecurity, also took Norse Corp to task, revealing that its insights into a malicious insider at Sony were nothing more than rumors and gossip. Weeks after Norse Corp asserted to the media that its analysis of the Sony hack indicated a malicious insider, the FBI released federal indictments against various North Korean hackers, proving Norse Corp's assertions were incorrect. Additionally, Norse Corp's threat intelligence map was found to be little more than basic Internet searches that had been repackaged to look like an attack map. Norse Corp's map was jokingly called the "Pew Pew" map within the cyber community space.

At the time of all its hype, Norse Corp stated that the data it used to feed its online attack map came from a combination of over 8 million sensors and honeypot systems that the company had meticulously put in place in more than 47 international locations to gather and collate a variety of enemy attack data. However, as soon as the company began to implode, essentially because there was too much money going out the door and not enough coming in, some departing employees noted that while

Norse Corp data was potentially valuable, the leadership of the company was not interested in investing in operationalizing that data. Those departing employees stated that the leadership was satisfied with the interactivity and visuals of the "Pew Pew" map. Following the company's collapse, the map's developers publicly stated that there were serious questions about the validity of the data behind the map itself.

Norse Corp went from being a cybersecurity company with the sky as its limit to gone overnight. But outside of the suspicious fundraising and founder shenanigans (which seems to happen with many companies in cyber), what factors sealed their fate? What sin did the company commit in the eyes of the industry that it should have known not to commit? Norse Corp simply did not heed the warnings from the most significant leaders and contributors in the small community that is cybersecurity.

For years, Norse Corp made it a point to go for broke against the advice of its own board members, several of whom came with deep experience in the cyber community. Despite constant gentle notifications from its own personnel and its partners that Norse Corp was not being well received by the broader cybersecurity community, Norse Corp blatantly disregarded the warnings and indications. It was about to be "outed" by an industry built by people who pride themselves on discovering weaknesses and vulnerabilities in both systems and businesses. Norse Corp could have cloaked its shady business dealings and fundraising behind the veil of VC financing, as many other companies have, and continued without much interruption, but it should have known not to pee in the small swimming pool that is cybersecurity. Amid all the questions, accusations, and constant barrage of conversations around the company's technology and the validity of its most prized offering, the attack map, the leadership at Norse Corp should have taken the time to step back and ask themselves, "Should we keep doing this the way we are?"

As with the parable of my own painful lesson about listening to the more experienced folks who are in the trenches doing the work, Norse Corp leaders never took a pause and read the room. Had they done that, they would have noticed the following:

- Employees were openly criticizing and questioning the company's product value.
- Most cybersecurity insiders were also poking at the weaknesses in the company's offering and public presence.
- The company received a frigid reception at industry events and conferences.
- The CEO and CTO had to publicly defend the value proposition of the "Pew Pew" map at every turn.
- At industry events, the company hired actors in full Viking regalia who were met with outright laughter.

Sure, if you look at the entirety of the cybersecurity space, you can find companies that have goofy marketing campaigns, and you can certainly find companies that aren't well received by the community. But Norse Corp set the standard, and at every turn, it chose to ignore the inputs it was receiving. If what your company is doing makes your employees feel as if the community they are selling to and serving in doesn't want them there, stop what you are doing and do something different. Immediately.

Knowing what to do is difficult on its own. Figuring out how your offering or product fits in an exceptionally saturated market is hard enough. But knowing what not to do and deciding on strategies to not do those things is often harder and often overlooked. Does your company have bloated and out-of-touch P&L methods? Stop using them. Change the method. Does your leadership disregard the inputs and valuable insights of the worker bees who know what the hell is going on? Listen to those people, and gain value from the knowledge *they* gained from their pain

and experience in the profession. Is your leadership not reading the room and paying attention to indications from the community and leaders in your space that their offering is not well received and, in some cases, is being probed by people who make their living finding weaknesses in systems? Don't continue down that path. If you want to grow your business smartly and be the best leader you can be, you should take a minute and ask yourself, "What shouldn't we do?" It may be the most valuable question you ever ask.