Why CISOs Fail
The Missing Link in Security Management—and How to Fix It

Barak Engel
Contents

Foreword ix
Preface xv
Acknowledgments xix
Author xxii
Praise for “Why CISOs Fail” xxiii

Chapter 0 Why? 1
Chapter 1 The Dismal Discipline 7
Chapter 2 The Business of Being CISO 25
Chapter 3 Let It Rain 43
Chapter 4 Don’t Call Me Sue 61
Chapter 5 Comply Oh My 75
Chapter 6 Techs-Mechs 97
Chapter 7 The CISO, Reimagined 117
Index 127
Foreword

In my 20+ years of adventures working, learning, and contributing to both the information security and intelligence communities, I can still say I have only met a handful of noteworthy leaders. I guess that’s to be expected since they say that true leadership is quite rare… but should it be? In the information security field, it seems more than rare. Security leaders seem almost non-existent. Is that because there aren’t people capable to lead in this space? I don’t think so. We see highlights of leadership all around the Information Security community. We see open-source initiatives such as Offensive Security’s freely available Kali Linux Distribution, which provides an all-in-one pathway for learning and performing penetration testing and digital forensics. We see SANS taking the lead on the quest to offer scalable advanced Information Security education. We can’t forget all the open-source tools, that have been pioneered, that inspire more than half the commercial technologies of today such as Metasploit, Bastille Linux, Tripwire, BeeF Framework, Bro, Security Onion, Snort, Suricata, Mozilla Defense Platform, OpenBSD, SELinux, and to name just a few.

And then you have our individual security leaders that literally believe in protecting our security (and sometimes privacy) communities and by boldly doing so create disruptive advances within our industry. The first one that comes to mind is security leader
Katie Moussouris, who used her skills to courageously stand up for hackers and security researchers and their misunderstood community by literally pioneering an entire industry for them. This allowed their abilities to be demonstrated and valued as a positive benefit instead of something to be feared. While she was at Microsoft, she creatively designed a solution to the very complex and long-standing problem of vulnerability research and disclosure management. Katie put in place bug bounty programs that incentivized hackers and big corporations to do the unthinkable and miraculously work together willingly. This solved not only the logistical problem of scaling vulnerability disclosure and management through hacking policy, but it tapped into the heart and soul of a human issue: the legitimate elimination of rejection the majority of hackers and security researchers encountered due to non-acceptance, fear, or misunderstandings. Through cooperative game theory strategy and a deep sense of empathy and ingenuity, Katie instead bridged that gap, and also created a freelance marketplace for hackers to thrive personally and professionally based on their skillset. A game-changing win–win. Katie continues to lead as the authority in vulnerability disclosure and bug bounties as an expert for the U.S. National Body of the International Standards Organization (ISO), and she led the charge in helping the U.S. Department of Defense start the government’s first bug bounty program.

There are a few others that have fought the good fight and created industry, or law, or policy. People like Phil Zimmermann and Jon Callas of PGP (Pretty Good Privacy) fame; we have folks like Richard Clarke and Howard Schmidt that championed cyber national security policies for the White House. Yet, the real rarity is the day-to-day leadership. The success of consistency without glory and fame. The required discipline to maintain the passion over the onslaught of politics. The reality that the leader serves the team, and not the other way around.

Now bring in the security aspect and then we have to not ignore the elephant in the room: the Information Security ego. We cannot deny it. Worse, it is encouraged in our community. The security leader, the CISO in most cases, is expected to know everything.

And that is why I am very excited that this boldly written yet extremely (maybe even aggravatingly) informative and much-needed work is finally here!
But first, a **word of warning**: before reading this book, you will need to leave that Information Security ego at the “LOGIN” prompt. Otherwise, you will not even come close to receiving the real game-changing insights this book can provide. I therefore implore you to go in as if you were a beginner in your field. Tap into the young ambitiously curious good old days where you didn’t see hard or easy, but only an opportunity. Go in with no preconceptions, and definitely don’t take the book personally unless it’s where you see you can personally apply and improve. Then get ready to gain a new perspective that may shift your thinking with great benefit to you, your organization and the constituencies that you serve.

On a personal note, I’ve had the honor of working with Barak Engel throughout my career. He has brought me a lot of opportunities I can truly say I wouldn’t have otherwise had, and more importantly those opportunities together provoked and invoked constantly new perspectives for me. These perspectives that Barak would impart literally impacted my career in such that it pivoted me from someone who excelled just as a technologist and advanced technical security geek to a balanced information security professional. He got me to think beyond the bits and bytes, which not only enhanced my logical-to-lateral thinking abilities greatly, but I also learned business strategy, social intelligence, perception management, and even political de-escalation techniques that to this day help me achieve the best success of managing risk by encouraging transparency and discouraging passive aggressive political plays within the organization. To put it bluntly, the successes I have had within the organizations I’ve worked with (e.g., Head of Cyber at Deloitte, as well as taking multiple companies to acquisition, running my own companies, and currently as Chief Scientist and acting lead handling risk management/Information Security for Flashpoint) regularly include the philosophies asserted in the book you are about to read.

This book isn’t about technology. It’s about getting away from it. It’s about not treating a symptom, but instead solving a problem beyond the vacuum of what we think is Information Security. Why is it that 20 years later we are still trying to solve the same problems that we didn’t solve back then? And then, only to find everything more challenging and disappointedly reactionary. If you’re bored at your job because of this, then you should be. Why, because that’s boring.
It’s not creative. It has no strategy. It has no element of ingenuity. It’s throwing the next promised technology at a problem in a tactically reactionary manner with no benefit and only added stress and frustration on you and your team, and actually… wait for it… added risk to the company.

If you’re ready to get out of that repeated rut, then this book nails it. If I had an analogy, CISO expectations today remind me of the business of medical doctors handing out the newest pharmaceutical medications to their patience until something sticks. This brute force mentality is not very hacker-like. It’s definitely not creative. It incorporates precisely zero strategy. And likely in the long run will produce limited success.

If this book had a subtitle, it should be: The De Facto Common Sense Strategy Guide for Organizational Risk Management. The way Barak brings this perspective surprisingly simplifies the over-thinking, over-working, and over-political life of a CISO by demonstrating how the security leader truly gets to be the leader, the advisor, the sage, and the arbitrator for the entire business itself. This shift of the role finally empowers the CISO to break beyond the political barriers, and lead with fury one’s vision of security and risk management to its success, from planning all the way to execution. It pulls the EQ out of the IQ and overlays them neatly so that one can see the pragmatic decisions that need to be considered, but while encouraging and enhancing the creative side of solving these problems more with people instead of just technologies.

For the financially savvy types, the insight in this book can literally lower your TCO when it comes to security management and monitoring costs by looking the what the real bottom line actually is… in other words, your people at their finest.

Who knew?

For the policy and compliance oriented, you are definitely covered. From effective approaches for scaling data classification to map to your current Information Security policies, all the way to business continuity development and ensured execution.

What I love the most about this book is the fact that it isn’t a book about being just a CISO, and how to be one and why they fail. It’s a book about leadership through genuinely learning to understand your people successfully. I’ll admit, my team and the people on it come
first and foremost. I’ve taken massive political hits to go to bat for my team, and I will continue to do so if required. This book’s most vital takeaway is in the fact that it doesn’t ignore the use of social intelligence or the actual psychology perspective of managing risk. Essentially, this book was written with heart and wasn’t really written for the CISO’s gain, but mainly for the teams you continue to serve.

It has been an honor to be asked to write the foreword to this book. Because this book is humbling... and caring... yet confident, creative, and courageous, the exact qualities required for leaders to evolve to what we truly could be.

I will leave you with one of my favorite quotes from Thomas Jefferson:

One person with courage is a majority.

Thank you Barak Engel for this book. Enjoy the read!

With honor

Lance James
Chief Scientist
Flashpoint
"We're looking for a CISO."

This phrase has become increasingly common these days. I hear it so often that seemingly not a day goes by without someone saying that to me, be it a recruiter, potential client, or frustrated colleague through LinkedIn.

I can't say that this is a bad thing. Clearly, finding yourself in what appears to be a maelstrom of demand is always a healthy thing for one's career prospects.

And yet, it is almost inevitable that, when I ask a few basic questions about the goals for the role, it transpires that they view it as some sort of “really smart guy” (women do go into security, but unfortunately, it appears like it is even rarer in Information Security than in other technology disciplines) who “can figure out what we need to do to protect our systems.”

Which, to clarify, means doing so with technology, more often than not as part of the IT (information technology) department.

One particular conversation I had took place in the offices of a very large technology firm and household name. The CIO, a sharp and lively fellow, asked me how I viewed the role of a CISO. I explained that I thought of it as a business partner to all departments. As someone who can help the organization understand and manage underlying risks in business operations, hidden liabilities, brand management, and service agreements. Someone who could also help uncover ways to promote the brand further by enhancing consumer trust, engaging externally with the customer base and the media on emerging issues like personal information privacy and portability.

He looked at me and said, “I like it, but don’t you think that the main role is to protect the company?”

I knew what he meant. He tried to get me to talk about technology. Firewalls, benchmarks, intrusion detection, immutable virtual containers.
I didn’t.

“Of course,” I answered, and then added, “But I think that protecting the company means all of these things and more.” Guessing where his mind was going, I added, “You see, as a CISO, I never focus on technology, because technology is implemented to serve a business purpose, not as a business goal unto itself. Even if your business is technology, your ultimate goal is still to sell as much of it as possible, isn’t it?”

He became increasingly uncomfortable.

They ended up promoting a technologist internally into the role of CISO, and from all I can tell, nothing has really changed, even though they were gasping for change.

The fact that security budgets are taking an ever-larger portion of IT budgets only serves to reinforce the notion that security is a technology problem. The challenge here is twofold: first, the mistaken notion that security problems are generally solved via technology; and second, the even more mistaken notion that security is part of IT in the first place.

It shouldn’t be.

A big reason why that is the case is simply that, when viewed in this fashion, security also tends to primarily serve as a business stopper. Security technology solutions are, by and large, focused on the prevention of something bad from happening. Distressingly, it increasingly seems like technology pros have come to understand security primarily in the context of confidentiality, which, even if all you do is follow the oldest established approaches to security, neglects integrity and availability (also known as the CIA model).

In reality, bad things don’t happen in a vacuum. Rather, bad things are allowed to happen because they are a byproduct of an environment and a mission that desires good things to happen. For example, running a successful business, providing healthcare services to the population, or promoting government engagement. Now place yourself in the role of a CIO who has to referee between supporting the sales executive, who is a powerful peer and is pushing for a technology-based enhancement that will drive sales growth, and the CISO, who is a direct report and who states categorically just how dangerous it would be to move forward.

Worse, the CISO is engaging in a chewed-up version of doom and gloom like countless times before and, as is usually the case, fails to propose any reasonable alternatives. To put the final nail in the coffin, the...
doom and gloom never actually seems to happen (and yes, I fully realize the missing word here is “yet”; bear with me, that’s part of the point).

Is it any wonder that the CIO will, by and large, choose to go ahead with implementation?

The truly sad part is that by now, the folks practicing security in these common kinds of hierarchies have learned what appears like a valuable lesson: as long as fear is marketed internally powerfully enough, they can get extra resources approved. And the most dominant fear, at least in companies that have not yet suffered an actual breach with all of its glorious consequences, is the one driven by regulatory compliance, or even compliance with private standards, like the Payment Card Industry Data Security Standard (PCI-DSS). If there is ever a phrase that retail and hospitality executives will come to loath more than “PCI compliance,” then surely it will involve devil worship. It is a stop button, a “you can’t do business” button, a constant frustration that they are apparently powerless to overcome.

Thus, welcome to the new motto in security: “management by compliance.” We will discuss this tragic turn of events at length in Chapter 5.

Another big reason for why security should not be managed within IT is even simpler: security problems are rarely, at their core, technology problems, even though they can often be addressed with the assistance of technology. Note that this is entirely different from saying that the problems originate with technology.

I realize the risk of making this statement. There is a sort of imagery, common in security circles, that implies their job is that of the guard in front of a castle; that they must design the best moat and gate and mantrap and other surrounding defenses—in the form of technology infrastructure—to protect what’s on the inside of the castle, which is sensitive company data. This visual, in many different forms, is repeatedly reflected in countless security training and instructions manuals, videos, and other forms of education, and is accepted (or even assumed) by default. In my recollection from the mid-90s, one of the earliest manufacturers of firewalls used a marketing slide evocative of this idea—of the castle, the gate, the moat and the alligators, and the guard who was managing all of that, in the form of the firewall, from
a keyboard. It was clever, an easily understandable analogy for anyone listening, and it certainly didn’t hurt Checkpoint’s fairly successful pursuit of world dominance, as is the wont of every technology firm.

And yet, in this day and age this approach is self-defeating, for two reasons.

The first reason is fetchingly described (at least if you like Mexican food) by my good friend and long-time security practitioner and expert, Steve Levinson, who likes to call it the “Hard Taco” problem—as in, crunchy shell, soft (and leaky) core. If you imagine the shell as your perimeter defenses and whatever is inside the taco as your data, the image becomes irresistible. It is also often discussed in the context of “defense in depth,” which tends to be misunderstood just as often (and just as happily miscommunicated by security vendors) as simply a gated system of somewhat similar technology solutions. For example, you will often hear a security manager describing the “defense in depth” strategy within the organization as essentially a series of network-based firewalls and intrusion detection systems combined with network segmentation. That is akin to calling the enforcement of multiple password controls “multifactor authentication.” Both are wrong, but they are wrong in a nonintuitive way, thereby making the error harder to avoid.

The essential idea behind the castle and the alligators is that if we protect ourselves from the outside world, we will end up doing just fine. It’s intuitive; after all, it’s easy to think of the world in this “us versus them” fashion, with the bad guys (those dang hackers) on the outside knocking on the doors trying to get in, but the reality of security is quite different. Internal and behavioral threats can be far more devastating than external ones, and may materialize in many ways, such as social engineering, inadvertent leaks, bribery, employee disgruntlement, and even a simple lack of interest in security because “it is an IT problem.” Sadly, once somebody with malicious intent has access (they are past the crunchy shell), they will generally and easily be able to expand that access and get at the targeted data (soft core).

We will discuss this more in Chapter 6, but there is a question I like to ask executives who are locked in the “security in IT” mindset, which is this: “think back to 20 or 30 years ago, when all your sensitive stuff could be locked in safes and file cabinets. How many of your employees had access to those materials?” The answer is always a version of “very few,” often accompanied by a nervous chuckle. And it is a telling
chuckle indeed because, in today's age, with the promise of the paperless office in the here and now, they can't tell anymore who can get to what and when, not even if they ask. But they do know one thing: the IT guy can access everything, and also controls who else has access. At least when a safe was physically broken into, you could tell immediately upon finding it that it happened (well, unless you're in one of those Le Carré novels, I suppose). Even that simple assumption isn't true in information security, where breaches are usually detected weeks, months, and sometimes even years after the fact, if they get detected at all.

The second reason is that security pros who emerge from the technology ranks are indeed incredibly smart, dedicated, and often selfless, for security is a thankless job. But there is another trait they usually share, which is a lack of business training and business operations experience. This leads to a tremendous disconnect because of their lack of context. It makes sense if you consider it. A very smart, highly technical person is asked to “protect the company,” but is generally limited by their insight into how the company (or any company) truly operates—foundational things like its business model and cashflows, sales and growth strategy, and so on—and instead, are buried in the IT hierarchy. Is it any wonder that they constantly seem to “miss the mark” and focus on the wrong things, while making endlessly dire predictions? Or that everything seems like a major threat to them? Worse, they know that if they screw up, it is their head that will roll before anybody else’s.

Is it any wonder that these folks can come across as paranoid, unpleasant, or even scary?

---

How Security Firmly Places Its Foot in Its Mouth in the Most Mundane of Ways

A Short Essay on a Boring Topic

Let's talk about passwords.

It's alright, go ahead. I will wait patiently for you to be done with groaning and rolling your eyes.

You already know everything there is to know about passwords. They need to be long, and complex, and rotated frequently, and all that jazz. After all, that's what 90% of the security professionals
insist is the only way to keep anybody safe. Heck, even journalists seem to get it, and that’s a seriously high bar to cross.

That this advice is generally wrong and is no more than a technological manifestation of a form of inertia is, well, not something we really want to discuss.

Or maybe you’ve evolved away from this. You’re up to speed on passphrases. You know what two-channel authentication means, you know your SSO’s and your revised NIST standards (took those guys long enough to get it, too). Good for you.

Do you think passwords are a good authentication mechanism in general?

Because they aren’t. They suck. It’s just that they were the earliest form that we could easily implement in a client-server topology, and they stuck around since then.

Alright, alright, let’s roll back for a minute here.

What on earth am I talking about?

Instead of trying to explain everything, let me start with an example and a little quiz.

Ready?
Do you go to Starbucks?

I know I do, even as whatever foodie there is in me cringes at my saying it. I’ll allow myself to insert a plug for Blue Bottle Coffee here in the San Francisco bay area. Now that is some awesome coffee.

Anyway, back to our example.

Do you use the Starbucks mobile app?

It’s kinda nifty. If you don’t yet, I recommend you try it. Not only does it allow you to order your specialized, custom version of your favorite drink,* you can do it in advance of getting to the store, thereby avoiding the lines. Plus it tracks all your stuff and gives you your free rewards with no effort. In fact, it’s a very well-designed

* If you ever want to buy me coffee at Starbucks, that will be an extra-hot tall flat-white with one Splenda. Just saying.
app with a fairly friendly user interface (UI). Clearly, a lot of money and effort was invested in developing it, and some very good UI people were involved.

So what does that have to do with this book?

I’m getting to it.

Let us now examine an area where Starbucks information security got involved. How do I know? Because they had to: it’s the payment section. Security had to be involved there, because it’s a critical portion of the app that deals with sensitive consumer financial information—their credit card accounts.

The way Starbucks works to collect information about you, such as your favorite drinks, rewards, and (clearly) behavior, is by assigning you an internal ID, which is simply the random number of your representative “Starbucks card,” or store gift card. This ID stores your cash balance, which is drawn against whatever method of payment you might wish to use.

In the most convenient case, you enter a credit card into the app, and reload a certain amount onto your Starbucks profile in advance. You can even set the app to autoload more funds from your credit card to your Starbucks profile whenever your balance falls too low on the latter. Or you can reload it manually yourself.

And obviously, when you attempt to run a transaction this way, the app will ask for your password to ensure that, indeed, it was you who issued the request to do so.

Are we good so far?

No, really.

I mean it. Are we good so far?

If you were anticipating that I was about to make a point, you missed it, because the point was already made.

Can you tell where?

It’s in the last sentence, about the need to enter your password. It is a classic example of an innocent, well-intentioned, security screwup.
How so?

It’s easy to see when we think of it, not from a security controls perspective, but from a human behavioral perspective.

I’ll ask you a simple question: when would you typically be attempting to reload your card?

If you are like most people, it will be at exactly the least convenient time to do so—that is, while en-route to or in line (or more likely, trying to avoid the line) at the store, while on your phone.

It’s human nature. That’s what we do.

So now the app is asking you to enter your password at the least convenient moment, when you are most hurried in its use. It’s annoying to even have to think about it, but there it is. It’s important to protect our credit card, after all.

Right?

So what is a loyal Starbucks customer to do?

You know the answer already. You pick a simple password that’s easy for you to remember.

And there it is. A well-intentioned security control that is divorced from situational human behavior has resulted in a weakening of the entire ecosystem of the Starbucks e-commerce platform—because, of course, that same password is also used to login to the main Starbucks Web site, where a lot more personal information and transactional capabilities about Starbucks customers are available to the enterprising collector of such curiosities.

There are many ways to solve this issue while both making it easier for the end-users and strengthening the overall security of the ecosystem (the thankfully increasingly prevalent two-channel approach using an SMS code sent to the phone is one), but one thing is fairly clear: there was some form of disconnect at the business level between the security group and the folks who designed the UI.

It’s clearly exhibited via this transaction flow.
And by the way, don’t get me wrong. I am not picking on Starbucks here. Heck, it’s probably my favorite “fast-food” chain. I go there all the time. I’m just using it as an illustration of a frighteningly common problem.

To illustrate the prevalence of this problem, let’s try another one. Time to pick on United Airlines, another well-known giant. Look at Figure 1.1.

This email arrived a couple of months before I started writing this book, and I found it so amusing that I had to capture it.

---

**MileagePlus**

**MileagePlus # XXXXX336**

Barak, PINs are going away.

**Update about your MileagePlus PIN**

To better protect your United MileagePlus® account, later this week, we’ll no longer allow the use of PINs and implement two-factor authentication. This will impact you in two ways when accessing your MileagePlus account:

1. If you contact United® by phone, you’ll be asked for your password when using the automated system or for your security answers when you speak to a United representative.
2. Your security questions will also be used as part of upcoming two-factor authentication to further protect your account—you’ll be asked to answer your security questions the first time you sign in from a device that we don’t recognize.

If you think you may have forgotten the answers to your security questions, we recommend that you sign in to your account and select new questions and answers now.

Thank you for being a MileagePlus member and for taking the time to update your account.

---

**Figure 1.1** Email received from United Airlines.
So, can you tell what the issue is?

It is basically different version of the same problem. Note the description in the first bullet: you would have to provide your password to the automated system when calling by phone… another example of a hidden inducement to pick a password that is easy to remember (and type in while, uh, driving).

And yet, it was supposedly designed this way in order to increase the security of the system!

When you extrapolate this at a large scale, you will easily see why “easy-to-remember” passwords are such an Internet scourge. And the sad part is that people are, effectively and indirectly, practically trained by security professionals to engage in unsafe practices, as these two examples among many, many others, show.

Worse, those same professionals then have the gall to blame people for poor password choices when their accounts inevitably get hacked.

It’s not the users’ fault.

It’s our failure as a profession, a symptom of lazy thinking, a lack of interest to engage with our nontechnical peers and the business itself that leads to this happening, over and over again.

This is on us.

Before we get back to our regularly scheduled programming, here are a couple of tips to keep in mind with respect to passwords:

1. If passwords are a necessity, remember that length matters more than complexity. A string of 15 zeroes is far more difficult to crack than a fully randomized 8-character string, when both are properly hashed and salted.

2. Passwords are typically not a good way to deal with authorization, especially if the type of transaction involved is predetermined. Starbucks could have easily opted for an easier method of authorizing a reload within the mobile app using a challenge token (such as an SMS), because the worst that would happen would be that the user’s credit card would fund that same user’s Starbucks profile.

3. If you insist on using passwords, maybe due to technical reasons, then do yourself a favor and use different ones in
different security contexts. The easiest method here is to, say, use a PIN in low-security settings, and a password in high-security ones. And by all means, drop the complexity requirement and force length instead (see point 1), and while you’re at it, please teach your users what a passphrase is.

This leads us to a third and last big reason that security is not a technology discipline, and it lies in the nature of the landscape that security professionals face. Technical security (operations) management is, by its very definition, a case of asymmetric warfare. It is a well-known reality that no security system is good enough to withstand all attacks, all the time. In the world of physical security, at least the cost of attack is higher; it will often involve some expenditure in equipment, maybe bribery and other techniques aimed at human compromise. There is also the risk of being caught, arrested, and punished. Both the attack and the response are essentially localized affairs.

In the world of digital security, the cost of attack is often minimal, detection rates are low, and legal and criminal prosecution is close to impossible due to cross-jurisdictional issues. Attacks can be distributed, coming in from all over the world including, lest we forget, the inside—even as the people executing them can physically be anywhere, and out of reach of the law. As such, a patient attacker has only to try enough times in order to be successful, because they only have to be right one time.

The poor schmuck on the other side can’t ever be wrong.
They literally have no chance.

That reality in itself can be quite depressing. But when reduced to the realm of technology management, it can feel downright fatalistic. There is never enough technology that one can buy to truly protect everything, but in a world where new attacks evolve much faster than the typical budget cycle, one apparently has to accept the reality that their job, career, and good name may be lost tomorrow, and there is pretty much nothing they can do about it.

And the fact is that most security managers, as we discussed earlier, have very little foundation to grasp what truly matters to the business due to their unfortunate lack of relevant training. This is a great way
to spread misery in ever greater amounts, and by now you can surely understand why I like to call information security the *dismal discipline*.

Is it any wonder that security managers often sleep so little, drink so much, or are otherwise the most cynical and least agreeable in the IT organization?

I think by this time that you will agree that, just like in that definition of insanity, continuing to think about security as a technology problem even when that idea is clearly bunk, is tantamount to insanity.

The email comes through from a friend who is a recruiter. “Barak,” he says, “I wonder if you could help me.” The email goes on to say that one of his big clients has decided to seek a candidate for the newly created position of CISO, and is struggling to find the right candidate. He was wondering if it was a problem with the job description. It ends with “I know you’ve been doing this for awhile… can you help tweak it please?” The current job description follows.

I skim through it, and find no surprises. It includes a list of hoped-for technology-related skills and expertise, some boilerplate about management experience, and a couple of desired educational credentials and certifications like a B.Sc. in computer science and a CISSP. In fact, it reads pretty much like a typical director of IT security position, albeit with a fancified title.

“This reads like a fancified Director of IT Security position,” I write back, and admit that “I’m a little confused, to be honest. What are they really looking for?”

He gets back to me right away. “Yeah, I know. They don’t know exactly what they want, except that the last guy who had the director role left unhappy. That’s why I am asking you for help.”

I call him. In a depressingly familiar conversation, I learn that the company feels that security is important—the board and the top executives read the news, breaches are scary, and they don’t want to be the next name in the headlines—and even though they have tried doing something about it, their experience has been somewhat disappointing. Nobody ever understood the guy running security, who never seemed to communicate well and kept...
spending money on “who knows what” while reassuring them that “everything was going to be fine,” while at the same time fostering a sense of urgency by adding “if only we buy stuff immediately.” Needless to say, nobody felt reassured, but they were all a little afraid of him, and of the news, and so he kept getting his way. What really threw them off, though, was that he never seemed happy—it was hard to believe everything really was fine when the person telling you that everything was alright constantly appeared constipated while saying it.

I have seen this play out countless times, in different organizations, of different sizes, in different verticals. Even in those verticals where the understanding of security as a risk management discipline—a critical insight—was practically built into the culture, like in financials, often the implementation of that insight was lacking, although in somewhat differing ways.

As a result, companies repeatedly and recurrently hire wrong. They will hire smart, experienced people, and then set them up to fail, frustrating them out of the job in a couple of years. Or they will hire not-so-great but confident-seeming people, and let them “do their thing,” which does little to improve the security posture in the organization, but does a lot to introduce needless processes that end up serving no end but their own existence, at a significant human resource cost.

Here are common thought processes that lead to this pattern, and a response to each one:

- Security is hard.
- *The truth:* Security is no harder than managing cash-flows or penetrating new markets. All are disciplines that require a particular expertise. It just so happens that information security, at present, has a lower number of established leaders because it hasn’t been around for as long, and it is highly related to a field (technology) that is evolving rapidly. But that doesn’t make it harder. Being a CISO is just as difficult (or as easy) as being a CIO or CTO—which is, incidentally, one more reason why they should be peers.
There is also another element at play here, which is the good ol’ profit motive. The security space is filled with vendors offering niche solutions, using FUD (fear, uncertainty, and doubt) and fantastical claims that only serve to keep security as unapproachable. We’ve been here before with technology. Yes, the Nineties, I’m looking at you.

- Security is a higher stakes game.
- The truth: A favorite statement of candidates to the position of CISO, this is not only wrong, but dangerous. So let’s set this one straight. Security is there to support the business in its highest stakes game—in the case of a for-profit enterprise, manufacturing product, obtaining and serving customers, and carving out market share. A security person who is focused on technology threats all day will never be able to properly analyze the risk inherent in everyday business decisions, and will likely become ever more conservative in their decision making. The end result? The company pays lip service to the security leader while ignoring them where it really matters, which in turn leads them to become even more paranoid, frustrated, and upset, which in turn drives everyone else to behave even more covertly so as not to piss them off... until it all breaks down, they quit (or get fired), and a new person comes on-board to start the cycle anew. In the meantime, processes do fail and the business ends up assuming more risk than necessary, because everyone is afraid of bringing in the security person to assess the really important decisions, since they always seem to slow things down significantly. Sometimes that can lead to a bad data leak, which can harm the brand. At this point, when asked for my opinion, I tend to dismiss the candidacy of any security practitioner for the role of CISO who uses the “higher stakes” argument.

- Security is part of IT.
- The truth: We just spent a few pages discussing this issue, so hopefully we are on the same page by now. I do want to add a thought here, though. For the purpose of this discussion, I will assume you provide some sort of service...
or product that directly targets consumers or business—a b2c or b2b type environment. Ask your prospective CISO who their most important partnership is with, outside of their boss or direct reports. There are the typical answers—CIO, CTO, VP Operations, and so on. Some go further and mention the CFO or Chief Counsel, which are highly important and show a deeper understanding of the role. But the best ones will say “everyone,” and when pressed, mention the heads of sales and marketing. I will explain later in the book why these are such important business partners to the security leader, and hopefully, your candidate will be able to do the same, and give you concrete examples as to how this partnership has worked for them successfully in the past.

- If we aren’t compliant, we’ll have to shut down our doors.
- If you haven’t heard that one or a variation thereof, and you’re a senior executive in any reasonably sized enterprise, then you are either (1) woefully behind the curve or (2) lucky to have one of the best security pros in the business working for you. If it’s the latter, I congratulate you. If it’s the former, please reach out to me. But most likely, you are in neither category, and you have heard it before. The truth is that even in places where such draconian enforcement measures of security standards and regulatory compliance are common—say, the NSA—there is almost always a lot of wiggle room even after things go bad. Yes, there are exceptions that prove the rule (such as CardSystems International, which eventually shut down after a massive 2005 breach). But for the most part, companies can and do survive breaches. This is not to discount the heavy cost of breaches, in both remediation costs as well as ongoing costs for years, and in particular, a burden placed on technology use that can easily have a direct impact on the company’s ability to grow. But using this kind of language isn’t helping anyone. Did it ever really convince you, deep down? Or if you said it, did you ever truly believe it? Or were you using it in frustration to get your way?
All of these—and other—surprisingly pervasive misconceptions about security inevitably drive toward one common result, which is a series of failed hires into security leadership roles that make nobody happy.

Instead, I would suggest that companies reconsider the role of CISO in a different light. A fair number of books and articles have been written on the practice of security as risk management. They would be right, with an important caveat: information security is about managing the business risk related to the use of technology (with respect to information), rather than technology risk directly. In this sense, the CISO is akin to the risk manager in a trading firm—they (should) have the enormous power and responsibility to stop business from happening, but it is a power they must learn to use very judiciously, or else they will become ridiculed by the business makers, and worse, ignored and overridden regularly in the decision-making process, even when they are completely in the right.

I would like, however, to take it one step further, and suggest that the CISO should be thought of as a business enabler. This was not always true, but as technology has become completely pervasive to every part of the business, it brings with it both tremendous risk and tremendous opportunity. The right kind of CISO can serve as a bridge between the needs of the business and the risks related to the use of technology in supporting those needs. It’s just like the CIO who is serving to translate those same business needs into applied technology that is the best way to support those same needs.

This may superficially seem to contradict my statement that security not being a technology discipline. But it is not so. A good security leader does not need to understand the nitty-gritty of the technologies in use, just like the CIO does not need to know exactly how to configure each system in their domain. For the CIO, their value is in the strategic sense of knowing how to most effectively direct their resources where their value is truly realized; the CISO fills a similar role in terms of risk.

But because the CISO understands those risks in a way that may be different from the rest of the executive team, they can also help detect and suggest opportunities to use technology—and information—in a way that could trigger new and profitable avenues for the business to pursue, without adding undue risk. Their training and ability to
balance risk and reward, and their proximity (if placed appropriately within the company structure) to the “piping” of the company, gives them this opportunity. Viewed this way, the CISO is an advisor to the business, rather than a technology savant.

As an example, I will bring up the case of a transactional platform company serving the retail vertical. This was when technologies like Web application firewalls (WAFs) were first coming to market, and were still considered both bleeding-edge and unproven. In working with the company’s business leaders and looking for a way to gain a competitive advantage in the space, we made the case that by adding this technology to the company’s offerings, we could attain three significant benefits: (a) we would dramatically enhance the security posture of the organization in a world where threats were evolving ever more rapidly; (b) with proper messaging, we could significantly enhance the company’s message in the marketplace; and (c) we would “future-proof” the company’s compliance posture, since compliance standards (in this case, PCI-DSS) were bound to catch up. Oh, and of course, there was—(d) we would repackage this service as a premium add-on, allowing the company to recoup its initial investment and possibly turn a small profit.

And it worked.

Of course, there was risk involved. Justifying an expenditure of this magnitude at the time was hard. But by collaborating with sales and marketing to test the waters with strategic customers, we were able to do it, and gain all those benefits. But do you notice one thing missing from the above description? There is no discussion of “what would happen if we didn’t.” No FUD was necessary. It was a case of security and business leadership coming together to examine a security-initiated business proposal, and ultimately accept it as good for the business and a potential growth driver.

Certainly, we gained a nice side effect of protecting technology assets.

Unfortunately, this is rarely the case. In fact, the most common “methodology” (if you will) of managing information security these days is by compliance targets. Retail and hospitality are indeed verticals where this is particularly pronounced, with PCI-DSS often being the sole dictator of security decisions; if it’s not in scope for PCI and the company can pass its audit without it... well, good luck.
getting funding. But it’s not just in retail and hospitality anymore. The PCI standard itself has now transitioned across boundaries to many other industries that are only peripherally involved with credit cards. Retailers, after all, have many vendors, and it has become standard practice to require PCI compliance documentation before services can be acquired. Healthcare organizations are, naturally, focused on security requirements in HIPAA. Banks, of course, have many regulations to contend with. Companies with European presence or dealing with EU residents must adhere to European privacy regulations (such as the new General Data Protection Regulation [GDPR]) or face the risk of fines up to 4% of their global revenue (not profit). And so on.

At this point, one might legitimately ask the following question: why is this bad? After all, increased data protection regulation, often coupled with increased scrutiny, can only be a good thing, right? It holds companies accountable.

And the answer is, certainly, it should. But it pretty much never works that way, as we will discuss in detail later on.

But for now, let’s focus our attention on the security leader’s business role.

**Uncomfortable truth:** If someone wants you bad enough, they will get you. Why do we insist on giving people an impossible job that will get them fired when they inevitably fail?