A Story about a Strategy for Aligning Security and the Business

PROJECT ZERO TRUST

GEORGE FINNEY

Foreword by John Kindervag

WILEY

Project Zero Trust

A Story about a Strategy for Aligning Security and the Business

George Finney

WILEY

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBN: 978-1-119-88484-2
ISBN: 978-1-119-88485-9 (ebk.)
ISBN: 978-1-119-88486-6 (ebk.)

Library of Congress Control Number: 2022938397

Cover images: © Alhovik/Shutterstock; © venimo/Shutterstock
Cover design: Wiley

Contents

About the Author

George Finney is a Chief Information Security Officer who believes that people are the key to solving our cybersecurity challenges. George is the bestselling author of several cybersecurity books, including the award-winning book *Well Aware: Master the Nine Cybersecurity Habits to Protect Your Future* (Greenleaf Book Group Press, 2020). George was recognized in 2021 as one of the top 100 CISOs in the world by CISOs Connect. He has worked in cybersecurity for over 20 years and has helped startups, global telecommunications firms, and nonprofits improve their security posture. George is also an attorney, but don't hold that against him.

Chapter 1
The Case for Zero Trust

It was still dark in the room, but Dylan couldn't sleep any longer. He looked at the clock. It was only 4:45—not enough time to go back to sleep but too early to actually get up. Dylan was starting a new job today. Maybe his dream job if things worked out. So what if he was a little anxious? He was also genuinely excited, and he hadn't felt that way about a job in a long time. Or maybe ever. He closed his eyes again hoping for another few minutes of sleep.

Dylan opened his eyes and turned back to the clock. It now read 4:46. He decided to get up instead of waiting for the alarm. His house slippers sat next to his running shoes in front of the nightstand. He slipped on his running shoes. He turned on the lamp and walked to the treadmill sitting on the opposite side of the room. He grabbed his right ankle with his right hand, stretching his quadricep, stretched the other leg, then hopped onto the treadmill.

He heard the warm tone of recognition as the treadmill scanned his face and loaded his profile. His three favorite workouts popped up on the curved LED screen. He tapped the fourth icon at the bottom, and he could see nine livestreams of runners from across the world. He picked the one on a beach in Costa Rica and began running. He could hear a whoop from several other runners following the livestream that he had gone on runs with before as they saw him join.

But then a funny thing happened: the livestream froze. Then instead of reconnecting him, the treadmill started to slow down to a safe speed, then stopped. The March Fitness logo appeared on the screen like when his Wi-Fi had gone out a few months back. Dylan stepped off the treadmill and checked his phone, but the Wi-Fi seemed to be working.

He decided to jump in the shower and start getting ready for work. After he had gotten dressed, he started his morning ritual of making his coffee and checking his email for any news alerts. Since he was starting at a new company, he had created an alert to send him an email whenever a news story about his new company, March Fitness, and the word "IT" or "outage" were mentioned. To his horror, his inbox was full of emails. His treadmill wasn't the only one that wasn't working. The whole company was down due to an outage. Worse, a cybersecurity reporter was claiming on Twitter that the company had just experienced a widespread cyberattack.

Dylan stood there, unable to move. How could this be happening? On his first day? An alarm was going off somewhere, and it took Dylan a moment to realize that it was his alarm clock. It was finally time for him to wake up.

There was still a chill in the air as Dylan ran up the steps of the headquarters building. In the center of the stairs was a giant running shoe made from a wire mesh with only the toe of the shoe attached to the slab of marble underneath. He walked through the revolving door, and more wire mesh shoes divided the length of the hallway, each in slightly different running positions, as though some giant had just run through, losing a new shoe at each point in its stride. The lobby to the headquarters of March Fitness ran the entire length of the building, separating the headquarters of the company into the north side and the south side.

The north side of the building is where all the executives of the company had their offices, along with marketing, HR, finance, and sales. The south side of the building was where the Information Technology offices were located, along with the research and development offices. Unlike when he had interviewed, there was no one at the security desk, and the security doors on either side of the building were propped wide open. There was a steady stream of what Dylan thought were interns sprinting north to south and south to north, all carrying crumpled up papers in either hand. This was a bad sign; if they had resorted to physical messengers, it meant that not only email was down but also instant messaging and the phone system. Or maybe they had taken the network itself down to prevent the attack from spreading further?

Since Dylan didn't know where he should report, he headed toward the south side because that was where he had interviewed. He naturally broke into a jog to keep up with the messengers, and although he was in good shape and his six-foot-two-inch frame meant his steps were longer than average, the messengers darted around him like he was standing still.

He passed a bank of elevators and went into a cubicle farm where 100 employees would have normally sat. Instead, all the monitors were dark, and each had a piece of paper taped to it that read, "Do not power on."

He followed the stream of breathless messengers to a conference room where he finally saw someone he recognized. Dr. Noor Patel, the Chief Information Officer, was sitting at the head of a conference table in the center of the room. Noor was wearing a black suit and white shirt, with her trademark black silk tie. At the opposite side of the table was Olivia Reynolds, the CEO and Founder of March Fitness. Everyone else at the table was wearing suits except for Reynolds, who was wearing one of March Fitness's own brand of running suit.

"Dylan?" a woman whispered into his ear. She had silently moved through the standing-room-only crowd that had gathered around the meeting and startled Dylan. She had dark hair and was almost as tall as Dylan and smelled like lilacs. She was holding a binder full of papers that read *Business Continuity Plan*.

"I'm Isabelle. . . I run the Project Management Office. Noor asked me to keep an eye out for you this morning. Heck of a first day." She turned to stand next to Dylan and watch the discussion going on at the center of the room.

She handed him his ID card, the retractable holder already attached. "You're lucky we printed this last week. Now the whole card reader system is down, just like everything else. We started seeing some unusual activity on the network sometime Sunday evening," Isabelle whispered to Dylan. "By this morning, things were out of control."

He pinned the ID card to his belt, "I'm guessing you guys took the network down as a precaution? Do they know what the cause is?"

"Good guess, Dylan. Actually, a number of computers seem to have been infected with ransomware. We're still investigating the cause, but the company is losing money every minute the network is down, so what they're focusing on now is the fastest way to get us back online."

Olivia Reynolds spoke softly, but everyone immediately stopped talking and turned to look at her. "How do we know this ransom isn't just some kind of scam?" she asked. "Even if we did pay them, how do we know they'll actually unlock our computers?"

"Ma'am," one of the suits next to Noor spoke up. Unlike Noor, his suit was wrinkled and didn't seem to fit quite right. "We see this issue come up frequently. There are scam ransomware actors out there. We can tell when this is the case, because they'll use the same bitcoin wallet for all their victims. In those cases, you'll see lots of transactions where their victims tried to pay up."

"That's our security consultant, Peter Liu," Isabelle clarified quietly to Dylan.

"And in our case?" Olivia asked.

"In our case," Noor responded before the consultant could answer, "the bitcoin wallet is brand new, with only one transaction that we believe was just the cybercriminal testing the account."

"How does that explain anything?" asked a white-haired man wearing a blue pinstripe suit.

"That's our General Counsel, Kofi Abara," Isabelle clarified. "He's one of the smartest people I've ever met. Also, he runs a monthly poker tournament. He was actually in the World Series of Poker a few years ago. Never bet against him."

"It's an accounting issue," Peter explained. "The cybercriminal needs to know which victims have paid and which haven't. The only way to do that is to have a different bitcoin wallet for each victim. Seeing that the bitcoin wallet is empty means this cybercriminal is serious."

"What's our next move?" Olivia asked.

Noor stood up and addressed the room. "We aren't going to pay this cybercriminal if we can avoid it. We have our backups, and our team will go into overtime bringing computers back online from scratch. We've delayed upgrading our antivirus to a more modern EDR solution, so we'll be doing these upgrades in parallel while we restore our devices. This will improve our visibility into systems to be able to detect and prevent further intrusions as well. Our consultants will be working with us to ensure the entire process will take hours, not days." There were cheers from around the room from nervous IT staff ready to get to work.

Isabelle leaned over to Dylan and asked, "What's an EDR tool?"

"It's like antivirus software on steroids," Dylan whispered. "It stands for endpoint detection and response. Old antivirus programs would use a kind of fingerprint to find malware, but the bad guys figured this out and would use different fingerprints. EDR works like facial recognition, so it doesn't matter if you grow a beard or put on glasses. It can also take action to kick the bad guys out."

Isabelle nodded thoughtfully as the conversation in the room settled back down.

"That sounds like a great plan, Dr. Patel, but what if it takes longer than you expect?" Kofi asked.

"Our cyber risk insurance company will continue negotiating with the cybercriminals on our behalf," said a blonde woman wearing a bright red suit. She nodded to several consultants who were standing up behind her. "They'll be working with the ransomware gang to reduce the ransom as though we intended to pay, to buy us additional time."

"That's Kim Self ," Isabelle added. "She's our Chief Risk Officer. I'll introduce you later." Noor spoke up again, this time flanked by two directors who had been taking her notes down on their notepads.

"If our restoration goes for more than 36 hours," Noor clarified, "working in shifts, then we'll recommend paying the ransom. But we expect to be fully operational again in three days."

"How much will that hurt?" Olivia asked, turning to look in Dylan's direction.

Dylan was startled when the pink-haired woman standing on the other side of him answered. "We'll be giving a free month of credit to all of our subscribers for the outage." Dylan could see her nametag read *Donna Chang, Chief Financial Officer*. "It will hurt the same whether it's a day or a week. We can handle it for now, but we need to start thinking about the long term. Customer melt is a concern. But frankly the bigger concern will be the recovery costs, which are still unknown."

Olivia stood up and addressed the room, "Thank you all for being here. I'm not going to lie, the coming days will be a challenge. We will get through this challenge. We will be stronger because of it. We'll meet back here at the same time tomorrow, and we'll keep the video conference going so check in if you have any updates before then. Also, make sure you have the cell phone numbers for the people on your team until we can get our phone system back."

The next several hours were a blur as Dylan worked to help whomever he could. But with no access and not much information about the network, there wasn't much he could do. He mostly became a gopher, picking up supplies and carrying them to admins scrambling to rebuild computers from scratch.

"There you are," said Isabelle, who was peeking over a cubicle wall. Dylan was under the desk, unplugging it to bring to an admin he was working with. He hit his head on the bottom of the desk as he came out.

"Please tell me you've got something for me to do? I've been carrying around computers all morning."

"Boss needs you." She was already walking away at a brisk pace, and Dylan had to run to catch up.

She took him back out into the lobby, past a giant sneaker suspended in mid-air, and into the north side of the building.

Dylan's phone buzzed in his pocket. He pulled it out. It was Chuck, the recruiter whom he had worked with to get the job here at MarchFit. He silenced the call and kept following.

The smell of espresso filled the air of the executive suite. It made Dylan feel even more alert than he already was. "Is that the original stand-up desk treadmill that Olivia invented?" Dylan asked as they passed several prototype desk and treadmill concepts before the TreadMarch+ that Dylan owned came out.

They walked by a tall conference room table that had small treadmills where each of the chairs would have been. "Walking meetings," Isabelle said. "We had several large clients ready to place orders before the pandemic hit."

Isabelle turned to smile at him, but kept walking. They arrived at a pair of bright orange double doors. Isabelle knocked and opened the door for Dylan.

He walked in, but Isabelle didn't follow. "Best of luck" was all she said as she walked away.

The office was framed by two walls of glass with a TreadMarch+ stand-up desk facing the windows. The third wall looked like a NASCAR garage, with red tool chests and work benches covered with power tools and treadmill parts in pieces scattered everywhere. In the center of the room was a small white table surrounded by four red, modern-looking couches. On the table was a stack of several binders. The one on top was the same one Dylan had seen Isabelle carrying earlier, the Business Continuity Plan.

"Is this the guy?" said an unfamiliar gentleman sitting on one of the couches. Olivia's office, Dylan finally realized. Noor was sitting with her arms folded across from Olivia, who was leaning on the top of her desk. Noor nodded yes in answer to the man's question.

"Tell me, Mr. Thomas, do you believe that the incident that just happened to MarchFit could have been prevented?"

Dylan looked to Noor and Olivia. Their faces were blank, apparently waiting for him to answer. This was a serious question.

"I don't really know enough about all our technology to answer . . ." Dylan responded, but was interrupted.

"This isn't a technical question. This is a philosophical question. Do you believe that prevention is possible?" The man had tented his fingers waiting for Dylan to respond.

"I suppose," Dylan began, "that we have to believe prevention is possible."

The man waited several seconds for Dylan to continue, then asked, "Why do you have to believe that prevention is possible, Mr. Thomas?"

"Don't you have to believe that success is possible in order to have success? If we didn't believe we could prevent cybercriminals from breaking in, we'd unconsciously make it happen. Also, I'd be crazy for making this my career and not believe I could make a difference."

"Next question. What's the purpose of cybersecurity?" the man asked, folding his arms.

Dylan considered. "Security is only here to enable the business to keep running smoothly." The man nodded wisely at this and was silent for a long time. "Was there another question?" Dylan asked, turning to Noor and Olivia.

"Last question," the man said. "Do you enjoy learning?"

"Sure," Dylan answered. "You have to love learning in IT. We're always learning about the next new advance in technology."

The man jumped up from his seat quickly, and before he knew it, Dylan was shaking his hand. "You're about to learn a lot," he said to Dylan. "He'll do," he said to Olivia and Noor, and began walking out the door. "I'll see you tomorrow, Mr. Thomas."

"I'm sorry about all of this, Dylan," Noor said, turning to Olivia. She sat down on the couch where the man had just been sitting and gestured for Dylan to sit across from her. Olivia sat down next to Noor.

"There's nothing to apologize for," Olivia countered. She turned to Dylan, beaming. "This is a huge opportunity, Dylan. I'm really glad to meet you. I usually meet all our employees, but I wish we were meeting under different circumstances."

"We could at least ask him first so that he knows what he's getting into," Noor said. "Dylan, I know you were planning on meeting your team today."

"I saw a couple of them already," Dylan responded.

"Yes. But obviously some things have come up," Noor said. "Don't worry, you're not being fired or anything. But since you've not been trained yet, or really had any orientation time, you're not going to be much help with the incident response." She picked up her coffee cup and took a long, slow drink.

"Now it sounds like I'm being fired," Dylan laughed nervously.

"Dylan," Olivia answered, "you're definitely not being fired. A few hours ago, I asked Dr. Patel here what the most cutting-edge security program was in the world. And Dr. Patel, you said?"

"Zero Trust," Noor answered.

"Do you know what Zero Trust is, Dylan?" Olivia asked.

He folded his arms and crossed his legs. "I've heard of it, but I don't know much about it. Isn't that just a marketing term for security companies?"

The two women looked at each other with a knowing glance. Dylan got the uneasy feeling that this conversation had happened already.

"I asked the question, and it turns out that one of the world's foremost experts on Zero Trust lives just a few minutes away from us," Olivia explained. "You just met him. He's worked with John Kindervag and Dr. Chase Cunningham, the two Forrester analysts who pioneered Zero Trust. His name is Aaron Rapaport, by the way, but I don't think he actually introduced himself."

"So, I'll be what, working for him now?" Dylan asked.

"Technically, you'll still be working for me," Noor corrected.

Dylan turned his head to the side. "Technically?"

"She means that for the next six months you'll have a dotted line reporting directly to me," Olivia said.

"Oh" was all Dylan could manage. "So this consultant is my Obi-Wan? He'll teach me the ways of Zero Trust?"

"Here's why I'm convinced Zero Trust will work for us," Olivia said, both to Dylan as well as to Noor. "I read that the president has issued an executive order requiring the government to adopt Zero Trust as a strategy for securing the government against other governments. When I talked to Aaron just now, he convinced me. Dylan, tell me why I'm convinced."

"If the government is adopting it, then it must be right?" Dylan said sarcastically. The three of them burst into laughter. Noor finally relaxed in her seat.

"No. I was convinced because it's actually a strategy for security. This is the issue that Noor and I have been debating. With any other goal or objective in our business, we've got a strategy for achieving it. Our goal in security is to prevent bad things from happening. I know we can go buy tools or implement more tech to add to security, but how do we know we're on the right track? In every other area of the business we have a strategy, and Zero Trust is going to be our security strategy moving forward."

"I'll be leading the incident response and recovery efforts," Noor explained. "But at the same time, we'll be launching a transformation initiative for all of the technology in the company to fully implement Zero Trust."

"You've heard that an ounce of prevention is worth a pound of cure?" Olivia asked Dylan. He nodded. "That's what I expect of Zero Trust. That's why Aaron asked you about whether you believe in prevention. We believe that prevention is the most efficient way of stopping breaches, and Zero Trust is the best strategy for implementing prevention in technology."

"That makes sense," Dylan said.

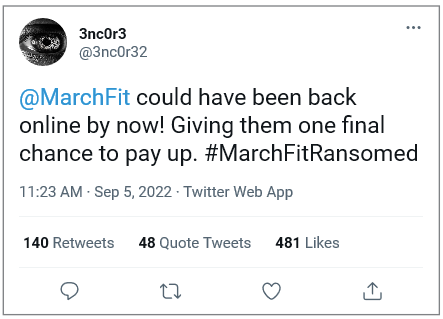
"This is a huge career opportunity. You'll be in charge of implementing Zero Trust at a company that's a household name. It would be crazy to turn this down," Olivia said, looking at Noor.

"So what happens in six months?" Dylan asked. "You said I'd just be reporting to you for six months?"

"In six months, we'll be launching a whole new product that will change the way the world looks at fitness, work-life balance, everything. We can't afford to make a misstep that could keep us from being first to market," Olivia said.

"We won't take for granted that you are on board with this new challenge, Dylan," Noor said. "You should take some time to think about this. You've specialized in managing IT infrastructure your whole career, and this is a different kind of challenge, and not one that you thought you had signed up for yesterday. I wouldn't expect you to just blindly accept an offer like this."

There was a soft knock at the door and a redheaded woman wearing a yellow suit came in without waiting for an answer. “Oh good, you’re both here,” she said as she approached Olivia and Noor. “We got a hit from our media monitoring service. The hacker has gone public with his demands.” She handed her phone to Olivia, while Noor and Dylan came closer so that the three of them could see the tweet from the cybercriminal.



A tweet from the cybercriminal 3nc0r3 publicly threatening MarchFit and confirming rumors of a cyberattack

“Dylan, this is April, our head of public relations,” Noor said. April reached out and shook Dylan’s hand.

“Who is this Encore person?” Olivia asked.

“His profile makes it seem like he’s based somewhere in Eastern Europe or Russia, but it’s not clear where he’s from. His past tweets indicate he’s ransomed several other organizations, but we’re the biggest target he’s gone after so far,” April explained, taking back her phone.

“I’ll check with the negotiator to see if this is the same person they’ve been talking to,” Noor said, standing up. “The negotiator was supposed to be stalling for more time. This could change our timeline.” She walked to the door, and Dylan followed before she stopped him. “You can take all the time you need to think about this, so long as you make your decision in the next few hours.” She winked at him. “Also, if you decide to be our Zero Trust project leader, you’re going to have a bit of homework before tomorrow.” Noor pointed to the stack of binders on the table.

Dylan began to walk outside. He was carrying one of Olivia’s designer backpacks heavy with all the paperwork he had to read. On the way out the door, he noticed MarchFit’s motto, “Every Step Matters,” written above the entrance to

the building. The fresh air helped, but what he really needed was to go for a run. The stress usually just melted away when he ran.

The job he'd be doing wasn't like anything he'd ever done before. It was an opportunity, but not the one he had been imagining just a few hours ago.

He unlocked his phone and remembered he had missed a call. He hadn't noticed that there was a voicemail, so he pressed the button and put the phone to his ear.

"Dylan, this is Chuck. Man, I know you just started over there at MarchFit and I heard about the breach. I just heard back from one of the other companies you were interviewing with at the same time as MarchFit and they're making you an offer. Dylan, it's more money and you'd be in a very similar role. If you think this thing is going south, give me a call and we can get you out of there."

Dylan collapsed onto the bench, exhausted. Things were moving too fast. He was too tired to think straight.

He looked up and saw a couple running together past the building. They waved as they passed by. Then more people ran. He realized the running trails that surrounded the headquarters building were full of runners. They were hooting their support every time one of the exhausted MarchFit employees would leave the building.

He hit the button to call Chuck.

"Dylan, hey buddy. I knew you'd be calling. You don't need to let this job set you back. . . ."

"Chuck, thanks for the offer, but I'm going to see this one through."

"Are you sure, man? Some companies don't do so well after a breach. I'm talking layoffs. I'm giving you a safe way out, bro. You could go be a director of cloud infrastructure anywhere. You're on your way to being a CIO soon. I'm worried this could hold you back."

"March Fitness got me through the pandemic, Chuck. You knew me three years ago. If I hadn't gotten that treadmill, I might not be here. I'm serious, losing all that weight has made a difference for me. I know it can make a difference for other people, and I'm going to stick it out here to make sure the company is still here to help other people."

Key Takeaways

Trust is a vulnerability.

Zero Trust is a cybersecurity strategy that says that the fundamental problem we have is a broken trust model where the untrusted side of the network is the evil Internet and the trusted side is the stuff we control. Therefore, organizations

don't do any real security on the trusted side. However, almost all data breaches and negative cybersecurity events are an exploitation of that broken trust model. Zero Trust is about getting rid of trust when it comes to technology. How much trust should you have in a digital system? The answer is zero. Hence, Zero Trust.

Zero Trust is a strategy for success when it comes to cybersecurity. The reason that Zero Trust resonates with presidents, CEOs, and other leaders is that they recognize that having a strategy for winning in any discipline is critical to success. Every company is different, which means that how a strategy is implemented will vary from one company to the next. A successful Zero Trust implementation will be custom tailored for each business to meet their unique needs, tools, and processes.

The primary goal of Zero Trust is to prevent breaches. Prevention is possible. In fact, it's more cost effective from a business perspective to prevent a breach than it is to attempt to recover from a breach, pay a ransom, and deal with the costs of downtime or lost customers.

Zero Trust is more than just a marketing buzzword. Zero Trust isn't any one specific tool that you can buy, because you can use many different tools to achieve the same objectives. Zero Trust isn't a reference architecture, because each implementation of Zero Trust will be completely customized.

Project Zero Trust will take you on the journey of a company that will successfully implement Zero Trust. You'll learn the most important concepts, methodologies, and design principles to take back to your own organization. For any strategy to work, you need to have some critical elements in place. March Fitness already had in place backups, a risk register, inventory, and a Business Continuity Plan (BCP) so they were able to recover rather than pay the ransom. They also had cyber risk insurance and already had contracts in place with a cybersecurity breach response service, and they were able to assist with the recovery and negotiations. And they had printed out all of their critical documentation on paper to ensure that it would be available even if their computers were offline. But even if you don't have these elements today, you can still adopt a strategy of Zero Trust.

Note that March Fitness has a Chief Information Officer (CIO) who also acts as their Chief Information Security Officer (CISO). Depending on the industry, many large organizations may or may not have a dedicated CISO or dedicated information security staff. Wherever your organization is at in its cybersecurity maturity, you can be successful at implementing a Zero Trust strategy. And if you haven't yet begun your Zero Trust journey, the best time to start is today.