TARKENTON

IDEAS AT WORK

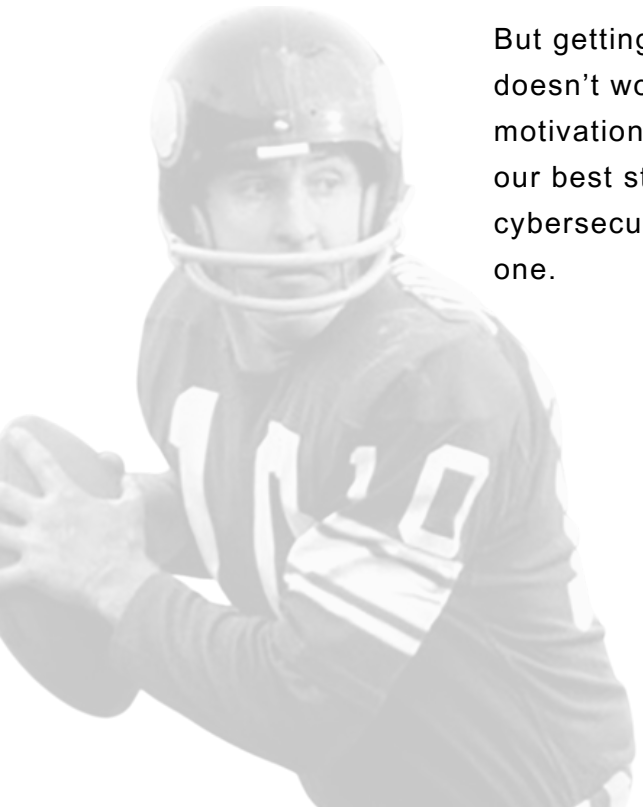
Now Is the Time: How to Motivate Your Team for Cybersecurity Training

Takeaways

- Lead by example in taking security seriously
- Avoid over-using fear as a motivator
- Patiently build a culture that cares about security over time

I've been part of a lot of teams. College football teams. NFL teams. Broadcasting teams. Business teams. One thing the best teams have all had in common is that everyone is fully bought in, from the top leadership all the way to the newest person on the team.

That's not just talking about buying into the goal – after all, every sports team wants to win, and every business team wants to succeed – but also buying into how we're going to get there. It's buying into the mission and vision.



But getting that buy-in isn't always easy. What inspires one person doesn't work on another, and we all carry our own interests and motivations. It's hard work, but it's worth it. This article from one of our best strategic partners applies this thinking to your company's cybersecurity. This topic is so important, you don't want to miss this one.

Now Is the Time: How to Motivate Your Team for Cybersecurity Training

It's no longer a matter of "if" your business gets hacked or falls prey to a cyber-attack. It's simply a matter of "when." Which means that NOW is the time to train your team on cyber-security practices and mindset. But how? It requires both making sure your team understands how cyber-attacks can unfold and then building a culture where everyone feels committed to protecting the safety of the organization.

Increasingly, cyber-criminals make a stealth attack that goes undetected for weeks, or even months. By that time, it's nearly impossible to get your money back.

An orthopedic practice in Florida with more than 100 employees learned this the hard way. The thief didn't breach their system; instead, he broke into the system of their medical billing partner, a company based halfway across the country.

The billing company had assigned a representative who worked directly with the controller at the orthopedic practice to collect fees. The hacker used the abundant data he stole from the billing company to "mimic" this representative, sending the orthopedic practice a "friendly reminder" email using an address with an almost-identical domain, requesting payment.

Without much fanfare, the orthopedic practice promptly paid the invoice – of $225,000. Unfortunately, that money went into the hacker's bank account, not the billing company's.

Another victim, a law firm with 20 employees, had recently hired a new attorney. In this case, the hacker infiltrated their system directly and mimicked the new lawyer's e-mail, asking the firm's payroll clerk to redirect his salary to a different bank account. "We've switched banks," he explained casually. "Could you please make sure my pay goes to this new account?" The clerk obliged.

It took months before the attorney realized he had not been paid. But there was no way to recoup those paychecks; they were long gone.

Some of these companies had cybersecurity coverage on their insurance policies, which offset some of the damage. Some ate the cost entirely. All of them lost money unnecessarily, because the bait looked *almost* right.

Many cybersecurity breaches seem like isolated incidents at first. Hackers break into your system and steal sensitive data. If you employ a cybersecurity expert or work with a partner vendor, they move in quickly to root out the thieves and re-fortify your firewalls. Then the intrusions stop. At that point, everything “seems” back to normal.

But hackers have become more patient, which means your entire team must be on alert and understand that "back to normal" might just be the calm before the storm.

The CEO of a VoIP company we know told a chilling story of how a hacker gained access to his company’s internal digital footprint and used the data to build a “profile” on the leader.

“I got a text message a few days after we’d cleaned up the breach,” he told us. “It read: ‘Do you want the hacks to stop?’ He proceeded to send me screenshots of my Social Security number, my credit report, the company cash flow projections, spreadsheets of where we stored all our usernames and passwords. I froze; my heart nearly stopped.”

It turned out, the thief had gained access to the company’s data by hacking the personal laptop of one of its remote employees, where he found all the usernames and passwords automatically stored by Google Password Manager.

You can imagine how many of us, owner and employee alike, rely on password management tools to avoid forgetting our credentials.

When all is said and done, you (and your employees) will pay a high price for ignoring cybersecurity training.

How to Motivate Your Team for Cybersecurity Training

A company where neither leadership nor employees cares much about cybersecurity is the most vulnerable. They are most likely to ignore or rebuff concerns about it, and pay the heaviest price when they’re hacked.

The optimal scenario for cybersecurity training is where both leadership and rank-and-file care deeply about protecting their company. The leader barely needs to mention it, because employees are self-motivated and spot villains quickly, taking immediate action. But to be sure, such firms are rare.

The vast majority of companies fall in the middle. The owner and perhaps top executives realize that cybersecurity training is a good idea. But to most rank-and-file employees, cybersecurity training feels like dental surgery: a good idea that nobody wants to do.

So, how do you get your team on board? Of course, having a training program in place is an essential first step, so don't ignore this. In our projects working alongside Tarkenton, we encourage every new partner to put proven, ongoing training in place immediately, if they haven't already done so.

Next, you need to be sure your employees take the training seriously, rather than treat it like just another boring HR video. While it might be tempting to threaten employees with locked accounts or terminations for ignoring their cybersecurity training, this rarely improves your security. It might achieve short-term compliance, but it will not yield a long-term, compassionate, and engaged sense of loyalty and duty, which is the only reliable way to make your cyber-security training pay off.

It’s also important to avoid over-using fear as a motivator. Stories like the ones we’ve shared here are good for getting the conversation started. But everyone becomes numb to fear, so this tactic won't produce lasting results either.

Therefore, the “quickest, easiest way” to an engaged, vigilant, and attentive team ... is also the slowest, most repetitive one.

Together with a cyber-security partner whose software has a proven track record (including clear, concise metrics on who’s taking cybersecurity seriously, versus who isn’t), you as the leader have some rounds to make on the floor.

Your goal: build and reinforce a culture in which your entire team truly cares about the welfare of the organization. This is not done overnight, but it will have myriad benefits beyond just cyber-security. Empowerment, transparency, positive reinforcement, and team building all help convince your team that cyber-security is a worthwhile goal.

The most direct path to a culture unified against cyber intrusion is forged by a chief executive willing to have constructive, compassionate and meaningful dialogue, many times over, with as many of their employees as necessary. It falls on you to spread the message: “This affects us. This will affect you. This will affect your co-workers. This will affect your families. What do you think is the appropriate thing to do?”

Foster this culture through repeated conversations, especially with the people whose training metrics reflect indifference. Seek their input, and ask them to tell you, in their own words, how they would respond to the threats you face if they were in your position. Then, reinforce the conversations through recurring, hands-on team building exercises.

Some cybersecurity providers and insurers now offer gamified “tabletop” exercises that help employees simulate an attack. In these scenarios, teams are pitted against one another in a friendly competition to respond to a breach. If your vendors offer this, don’t underestimate the power of routine security drills. As Seth Godin says, “We remember what we *rehearse*.”

We work with Tarkenton to guide business leaders through the conversations that can help build a culture of vigilance and shared responsibility, and help you find resources and partnerships to protect against cybersecurity threats. We’d love to help you, too.

By: Eric Bucher
CEO, QIT Solutions

Eric Bucher is the CEO and Co-Founder of QIT Solutions, providing MSP (Managed IT Services) with a cyber security first posture. "My leadership team and I believe in people above resumes; skills can be taught, but personality cannot. We hire individuals that are looking for a home, not for a job. This results in an outstanding customer experience for our clients, a team that supports each other, and individuals striving to improve continuously. While any MSP can offer managed IT services, QIT goes beyond by delivering a team of compassionate individuals who truly comprehend what it means to walk a mile in the customers shoes."