00:04

Today, I'm going to talk about a shameful topic. This has happened to many of us, and it's embarrassing, but if we don't talk about it, nothing will ever change. It's about being hacked. Some of us have clicked on a phishing link and downloaded a computer virus. Some of us have had our identities stolen. And those of us who are software developers might have written insecure code with security bugs in it without realizing it. As a cybersecurity expert, I have worked with countless companies on improving their cybersecurity. Cybersecurity experts like me have advised companies on good cybersecurity practices, monitoring tools and proper user behaviors. But I actually see a much bigger problem that no tool can fix: the shame associated with the mistakes that we make.

00:58

We like to think of ourselves as competent and tech savvy, and when we make these mistakes that can have a really bad impact on us and our companies -- anything from a simple annoyance, to taking a lot of time to fix, to costing us and our employers a lot of money. Despite billions of dollars that companies spend on cybersecurity, practitioners like me see the same problems over and over again. Let me give you some examples.

01:26

The 2015 hack of Ukrainian utilities that disconnected power for 225,000 customers and took months to restore back to full operations started with a phishing link. By the way, 225,000 customers is a lot more 225,000 people. Customers can be anything from an apartment building to an industrial facility to a shopping mall. The 2017 data breach of Equifax that exposed personally identifiable information of 140 million people and may ultimately cost Equifax something on the order of 1.4 billion dollars: that was caused by an exploitation of a well-known vulnerability in the company's customer consumer complaint portal.

02:13

Fundamentally, this is about technology and innovation. Innovation is good; it makes our lives better. Most of the modern cars we drive today are fundamentally computers on wheels. They tell us where to go to avoid traffic, when to take them in for maintenance and then give us all kinds of modern-day conveniences. Many people use connected medical devices like pacemakers and glucose monitors with insulin pumps. These devices make these people's lives better and sometimes even extend their lives. But anything that can be interconnected can be hacked when it's connected. Did you know that the former US Vice President Dick Cheney kept his pacemaker disconnected from Wi-Fi before he received a heart transplant? I will let you figure out why.

03:02

In a digitally interconnected world, cyber risks are literally everywhere. For years, my colleagues and I have been talking about this elusive notion of cybersecurity culture. Cybersecurity culture is when everybody in the organization believes that cybersecurity is their job, knows what to do and what not to do and does the right thing. Unfortunately, I can't tell you which companies do this well, because by doing so, I would put a juicy target on their backs for ambitious attackers. But what I can do is make cybersecurity less mysterious, bring it out into the open and talk about it. There should be no mystery or secrecy within an organization. When something is invisible and it's working, we don't know that it's there until it's not there. Kind of like toilet paper. When the COVID-19 pandemic began, what has been there all of a sudden became super important because we couldn't find it anywhere. Cybersecurity is just like that: when it's working, we don't know, and we don't care. But when it's not working, it can be really, really bad.

04:14

Toilet paper is pretty straightforward. Cybersecurity is mysterious and complex. And I actually think it starts with the notion of psychological safety. This notion was popularized by an organizational behavior scientist, Amy Edmondson. Amy studied behavior of medical teams in high-stakes situations like hospitals, where mistakes could be fatal. And she found out that nurses were not comfortable bringing up suggestions to the doctors because of the fear of questioning authority. Amy helped improve medical teams to make nurses more comfortable bringing up suggestions to the doctors for patient treatment without the fear of being scolded or demeaned. For that to happen, doctors needed to listen and be receptive -- without judging. Psychological safety is when everybody is comfortable speaking up and pointing things out. I want cybersecurity to be the same. And I want cybersecurity practitioners to be comfortable bringing suggestions up to senior executives or software developers, without being dismissed as those people who continue to talk about horrors and errors, and say no. Not doing so is really hard for the individuals who are responsible for the creation of digital products because fundamentally, it's about their pride and joy in their creations.

05:38

I once tried talking to a senior software development executive about the need to do better security. You know what he said? "Are you telling me we're developing insecure code?" In other words, what he heard was, "Your baby is ugly." What if instead of focusing on what not to do, we focused on what to do? Like, how do we develop better software and protect our customer information at the same time? Or how do we make sure that our organization is able to operate in crisis, under attack or in an emergency? And what if we reward good things that people do in cybersecurity in some way and encourage them to do so, like reporting security incidents, reporting potential phishing emails, or finding and fixing software security bugs in the software that they develop? And what if we tied these good security actions to performance evaluations to make it really matter?

06:35

I would love for us to communicate these good cybersecurity things and encourage them in some sort of company-wide communications like newsletters, blogs, websites, microsites -- whatever we use to communicate to our organization. What if a company announced a competition for who finds the most security bugs and fixes them in a two-week development sprint and then announces the winner of the competition for the quarter at a large company virtual town hall, and then rewards these people, these winners, with something meaningful, like a week's vacation or a bonus. Others will see the celebration and recognition, and they'll want to do the same.

07:15

In the energy industry, there is a really strong culture of safety. People care about this culture, are proud of it, and there is a collective reinforcement of this culture to make sure that nobody gets hurt. One of the ways they exhibit and keep this safety conscious culture going is by counting and visibly displaying days since the last safety incident. And then everybody works really hard not to have that count go back to zero because that means that somebody did get hurt. Cybersecurity is the same as safety. What if we all agree to keep that count of days since the last cybersecurity incident going on forever and then work really hard not to have it reset to zero?

07:59

And then certain things are a no-no, and we need to clearly communicate to our organizations what they are in an easily digestible and maybe even fun way, like gamification or simulations, to make sure that people can remember this. And if somebody does something they're not supposed to do, they should face some sort of consequences. So, for example, if an employee buys equipment on Amazon or eBay or uses personal Dropbox for their company business, then they should face some sort of consequences. And when this happens, executives should get the same treatment as regular employees, because if they don't, then people won't believe that it's real and will go back to their old behaviors. It's OK to talk about mistakes, but just like a teenager who violates the rules tells us about it, we appreciate that they told us about it, but there should still be some sort of consequences.

08:51

Cybersecurity is a journey. It's not a destination, and we need to keep working on it. I would love for us to celebrate cybersecurity people like the heroes that they are. If we think about it, they are firefighters, emergency room doctors and nurses, law enforcement, risk executives and business strategists all in the same persona. And they help us protect our modern life that we like so much. They protect our identities, our inventions, our intellectual property, our electric grid, medical devices, connected cars and myriad other things. And I'd like to be on that team. So let's agree that this thing is with us to stay, let's create a safe environment to learn from our mistakes, and let's commit to making things better.

09:39

Thank you.