Why Cybersecurity Is So Complicated

When you think of problems people had with cell phones back in the 80s, whether you experienced them firsthand or you've seen clips from movies, you know that it's a completely different mobile world we live in today. That seems to be the case with most tech industries — regardless of the problems that first appear, they all get eliminated eventually until we are living in a completely different world.

That being said, how come that hasn't happened in the world of cybersecurity?

When I first got into this crazy industry, people would reach out to me asking for my help with viruses, phishing attacks, criminal hackers, malicious employees and other such things. If we fast-forward to 20 years later, what are people asking for my help with now? You guessed it — viruses, phishing attacks, criminal hackers, malicious employees and other such things. All the same problems we had 20 years ago, plus so many more.

Why does it seem like all other tech industries get better with time, but the problems associated with cybersecurity only seem to get worse? I believe there are several reasons for this. Before tackling any cybersecurity strategy, it's important to understand what those reasons are and what makes this industry so different. I'm going to break down four of those differences here:

The Human Element

When organizations need to come up with a cybersecurity strategy, part of what they need to protect are their people. This can be incredibly challenging, as numerous digital forensic assessments that I have personally been involved with prove that people keep getting tricked into doing things they shouldn't be doing. Imagine trying your best to build an impenetrable house for the sole purpose of protecting your family from bad guys. It would make it pretty difficult to do your job if it was your family that kept letting the bad guys in. That is what's happening with cybersecurity.

Things Keep Changing

If I was to tell you in the 90s I wanted to talk to you about corporate security, you would've thought I was referring to video cameras and security guards, but as we changed the way we did business, we had to change the definition of corporate security. Over the years, we threw around terms like mobile security, cloud security and hosted security. And every time we thought we had a handle on our cybersecurity strategy, things would change. We'd put data somewhere new and we'd have to rethink our cybersecurity strategy. Now data is everywhere: in our toasters, our picture frames, our jewelry — you name it, it's there. And if it's not there yet, it certainly will be eventually, and the more places that contain data represent more places that need to be protected.

Government Involvement

There was a time that the government had no involvement with how an organization chose to run its cybersecurity program. But in the early 2000s, governments took basic security fundamentals and converted them into regulations and, in some cases, laws. This complicated matters for organizations, as compliance creates an additional business risk.

Take a look at what happened to Uber. Cybercriminals got the company to pay $100,000 via a cyber ransom, but because Uber had failed to follow proper breach notifications, the U.S. government fined it $148 million.

The Evolution Of Crime

Yes, malware codes and social engineering tactics have gotten more advanced over the years, but I'm not even talking about that. What's more important to note is the reasons for carrying out cyber breaches have evolved.

What I mean is, 20 years ago, when I used to get calls from organizations telling me they had fears in regard to cybercrime, one of the biggest concerns was a cybercriminal defacing a corporate website. That's what criminal hackers did back then. They would come home from their legitimate jobs, then they'd start their hacking, and one of their preferred crimes was to breach a corporate website and vandalize it for bragging rights.

But then those hackers started to realize that they could actually make a lot of money doing this, so there are no longer part-time hackers looking for bragging rights; rather, what we see now are fulltime criminal hackers working to support organized crime or even state-sponsored attacks.

The fact of the matter is that the problems associated with cybercrime and cybersecurity are here to stay and will most likely continue to get worse. These issues are alive and are not something we can just pass on to the IT department. Cybersecurity is a C-suite issue that requires corporate-wide attention regardless of the size of your company.

We need to understand our vulnerabilities in this digital world, and we need to understand what risks those vulnerabilities expose. Once we understand those risks, we can begin to understand them in economic terms so we can prioritize our strategies based on financial impact.

By Danny Pehar