Microsoft's security chief explains why the company is eliminating passwords

Kate Fazzini | @KateFazzini Published 16 Hours Ago Updated 16 Hours Ago CNBC.com Bret Arsenault has been Microsoft's top cybersecurity official for a decade. He talked to CNBC on the perils of the role, making quick decisions and the surprisingly simply steps companies can take to be more secure. Cybersecurity officials need to be seen by the board of directors, he said, in order for any effective initiatives to work.

Microsoft

Bret Arsenault has been the top cybersecurity executive at Microsoft for ten years.

It was 4 a.m. on a night in June 2017. Brett Arsenault, the top-ranking cybersecurity executive at Microsoft, had fallen asleep on top of his

cell phone when it shocked him awake with a buzz.

A cyberattack, later dubbed NotPetya, had begun locking down computers and shutting down businesses in Ukraine.

It first looked like a routine ransomware attack, in which companies would have been able to pay to open their locked up computers. But NotPetya was different -- it spread lighting-fast, like a worm rather than ransomware, and companies quickly found there were no criminals to negotiate a ransom with at all, leaving them with inoperable hardware and no data.

Arsenault quickly jumped on a phone call with staff in Eastern Europe and the U.S. He demanded his staff shut off access to Ukraine within 10 minutes to stop the malicious software from spreading out of Microsoft's locations in that country.

The staff said they didn't think they could do it that fast. He pushed. They worked. They shut it down.

"If you do the right thing, they'll say you did your job. If it's the wrong thing, you get fired," said Arsenault, Microsoft's chief information security officer. "It was my team trying to not call chicken little. That is probably the hardest part of the job, to not get overexcited but not to under-react."

He might have the hardest cybersecurity job in the world, being accountable to the board of one of the world's largest tech companies, which supplies ubiquitous products and software that serve most other companies across the globe.

Microsoft is one of the most-attacked companies in the world. But Arsenault said the lessons he's learned from NotPetya and the other 6.5 trillion incidents the company sees each year can be used by businesses with much smaller profiles, and even by individuals. The biggest one: Get beyond passwords.

The simplest, oldest attacks are still popular

Microsoft is just as inundated with spam email, scams and phishing as its clients. These schemes still make up the bulk of most attacks, Arsenault said.

Email-based and password-based hacking underlie everything from the simplest frauds to the most complex, multi-faceted hacking campaigns, he said.

"We all sort of declared years ago that identity would be our new perimeter. People are very focused on taking advantage of identity, it's become a classic: hackers don't break in, they log in. I see that as a huge, huge thing for us to work on," he said.

"Password spraying" is an old-school method, where an attacker tries to access a huge number of accounts at once using some of the most commonly used passwords. It's simple but effective, especially where organizations don't have additional ways to authenticate their employees.

Once an attacker is able to gain access to a network through just one employee identity with one commonly used password, he or she can begin to do more damaging work, like stealing corporate information or impersonating employees to execute a financial scam.

"The reality is, we still see a lot of attempts of people trying to password spray. The best way to protect against the password spray is to just eliminate passwords. If you have passwords, you have to enable multi-factor authentication" -- that is, using a password in combination with another form of identification, like a random set of numbers texted to the user's phone.

"And so the thing that we are seeing is lots and lots of people just focused on eliminating that whole vector."

Passwords, by themselves, are useless

Ninety percent of Microsoft's employees can log on to the corporate network without a password, Arsenault said. It's a reflection of the "passwordless future" Microsoft has touted for years, and backed up by products to move consumers away from memorizing strings of confusing terms.

Instead, Microsoft employees use a variety of other options, including Windows Hello and the Authenticator app, which provide other alternatives for logging in, like facial recognition and fingerprints.

Microsoft is one of the few companies looking to eliminate passwords entirely, but other tech giants are also trying to help clients reduce their dependence on them.

For instance, Google has been testing stronger alternatives to passwords alone, like its USB key fobs which plug into customers' computers and provide a second factor of authentication for logging in. Google said last year this method reduced successful phishing attempts against its own employees completely.

Cisco is also banking on a future beyond simple passwords, after acquiring dual-factor authentication start-up Duo last year.

Cyber execs need to talk directly to the board

For companies with strict rules around identity, passwords and employee access, it can be difficult for cybersecurity executives to make any kind of change. That's where organizational structure plays a role, he said.

For top cybersecurity executives, there is a common trope, backed up by some data, that their tenure will usually last about three years and will often end when their company has had a breach.

Arsenault has lasted a lot longer: He's been at Microsoft since 1990 and held the CISO role since 2009. He said the short-term thinking of many companies on cybersecurity can be exacerbated by the short-term tenure of their CISOs. Gaining a longer term relationship with senior management, and especially the board of directors, is essential to make the kind of rapid change necessary to fight new threats.

He also notes that Microsoft has embraced a popular security model among tech companies: federated cybersecurity. This means that each Microsoft product has its own head of cybersecurity, focused more keenly on building security into the specific product and answering to customer issues.

"We have a similar federated model for red-teaming," he said, referring to the process of allowing ethical hackers to actively attack the company's networks and products to test for flaws. "We also do a third tier of external threat testing, for 'non-actualized' threat, or the ones

that look like the things that we want to go and address." This way, he said, the company can anticipate the next large scale attack like NotPetya -- and figure out a response -- before it happens.