

HOME > SECURITY

SECURITY [CARTECH](#) [APPS/SOFTWARE](#) [BUSINESS TECH](#) [GOOGLE](#) [APPLE](#)

Is Hardsec the Future of Cybersecurity?



[Ernest Hamilton](#), Tech Times | 09 March 2021, 10:03 pm



(Photo : Is Hardsec the Future of Cybersecurity?)

Malicious cyber activity is big business - it costs the US economy more than \$5 billion annually. According to the US Council of Economic Advisors, this figure is expected to exceed \$6 trillion globally by 2021. In 2019, over 7.9 billion data breaches were [reported](#), twice the number of cases seen in 2018. These worrying statistics make cybercrime more profitable than the global trade of all major illegal drugs combined.

MOST POPULAR

-  [China Chang'e 5 New Moon Water Discovery Can Help Create Permanent Human Presence](#)
-  [NASA's Hubble Space Telescope Spots White Dwarf](#)



"The good guys are getting tired," said Charles Carmakal, a senior vice president at [FireEye Inc.](#), the Milpitas, California-based cybersecurity company.

Despite the billions invested in securing our information, hacking remains a lucrative and attractive business. According to New York Times reporter [Nicole Perloth](#), hackers are able to make large sums by simply scouring systems looking for flaws in code that might allow backdoor entry to information. Once found, hackers are able to sell access to these bugs for six-figure sums.

Software bugs can and have been found in almost every commonplace application, from Apple's App Store, to Microsoft's PowerPoint. "Even anti-virus products - the very software designed to keep spies and criminals out - can be turned into a powerful spy tool", explains Perloth.

Therein lies the fundamental problem with cybersecurity: all software, no matter how sophisticated, is vulnerable to hacking. The US remains open to cybersecurity attacks because most organizations still rely on software alone to secure their data.

Part of the current software model is to use updates (known as "patches") to eliminate vulnerabilities as they are discovered. But distributing and uploading the patches themselves can be a vector for attackers to access systems.

The fantastic flexibility of software is what makes it great for powering our gadgets and performing complex functions. But that same flexibility is the Achilles heel in today's IT environment - as any software can, by definition, be rewritten.

According to Dr. Ronald Indeck, Former Director of the Center for Security Technologies at Washington University and CEO of [Q-Net Security](#), "none of the software-based systems are provably secure. If anything, cybercriminals can easily compromise such systems using malware programs such as virtual rootkits".

A new approach?

Hardsec - or Hardware-Based Security - is an emerging security approach that relies on physical hardware rather than digital software to secure information. A physical device that holds no software cannot be changed and is thus essentially 'hack-proof'.

"Provable security is only possible with something that is 'immutable,' that is, something that can't be changed," adds Indeck.



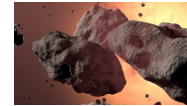
[Tesla Increases EV Prices in the US Again As High As \\$6,000! Model Y, X, 3 Included?](#)

4.



[Top 5 Best eCommerce Personalization Software to Increase Conversion Rates in 2022](#)

5.



[Ryugu Asteroid Rock Samples: Analysis Brings Initial Results, Scientists Awe in Amazement](#)

Subscribe to Tech Times!

Sign up for our free newsletter for the Latest coverage!

Email Address

[Sign Up](#)

that power our devices and can perform a wide range of tasks, FPGA chips can only perform a precise range of functions. They don't run any software and can only be programmed using specific physical pins, essentially making them "too dumb to hack."



Installing 'unchangeable' devices at all endpoints means every packet of data can be checked at lightning-fast speeds, securing point-to-point communications and ensuring malicious threats cannot spread across a network. This technology is also considered 'quantum-resistant'- impermeable even to futuristic quantum computing technology.

Hard-Sec has been the recommended standard by many cybersecurity experts - including the NSA - because it eliminates the need to use software vulnerable code, without reducing performance or slowing down the system.

What is the future for Cybersecurity in the USA?

As the COVID-19 crisis has forced more organizations to move their operations into the virtual space, cyber attacks will only become more lucrative. The Statista Research Department forecasts that the amount of data stored online centers has increased six-fold in the last five years. This data is primarily secured digitally, and consequently remains vulnerable to hacks.

For evidence of our ongoing failure to secure vulnerable data, look no further than the string of recent cyberattacks, like last year's attack on IT firm [SolarWinds](#), which affected several US Government Agencies, including the State Department and Treasury. This attack was so sophisticated that [experts admit](#) that it will take months to understand the full extent of it. Similarly, a sophisticated strain of ransomware called [Maze](#) hit dozens of companies stealing crucial data, including sensitive medical information from patients during COVID-19.

It is no longer good enough to simply rely on anti-virus programs and the never-ending cycle of software updates and patches. All organizations - particularly those tasked with protecting personal identifying information - have an obligation to embrace [hardware-based security](#) to finally get ahead of malicious attacks.

© 2021 [TECHTIMES.com](#) All rights reserved. Do not reproduce without permission.

Tags: