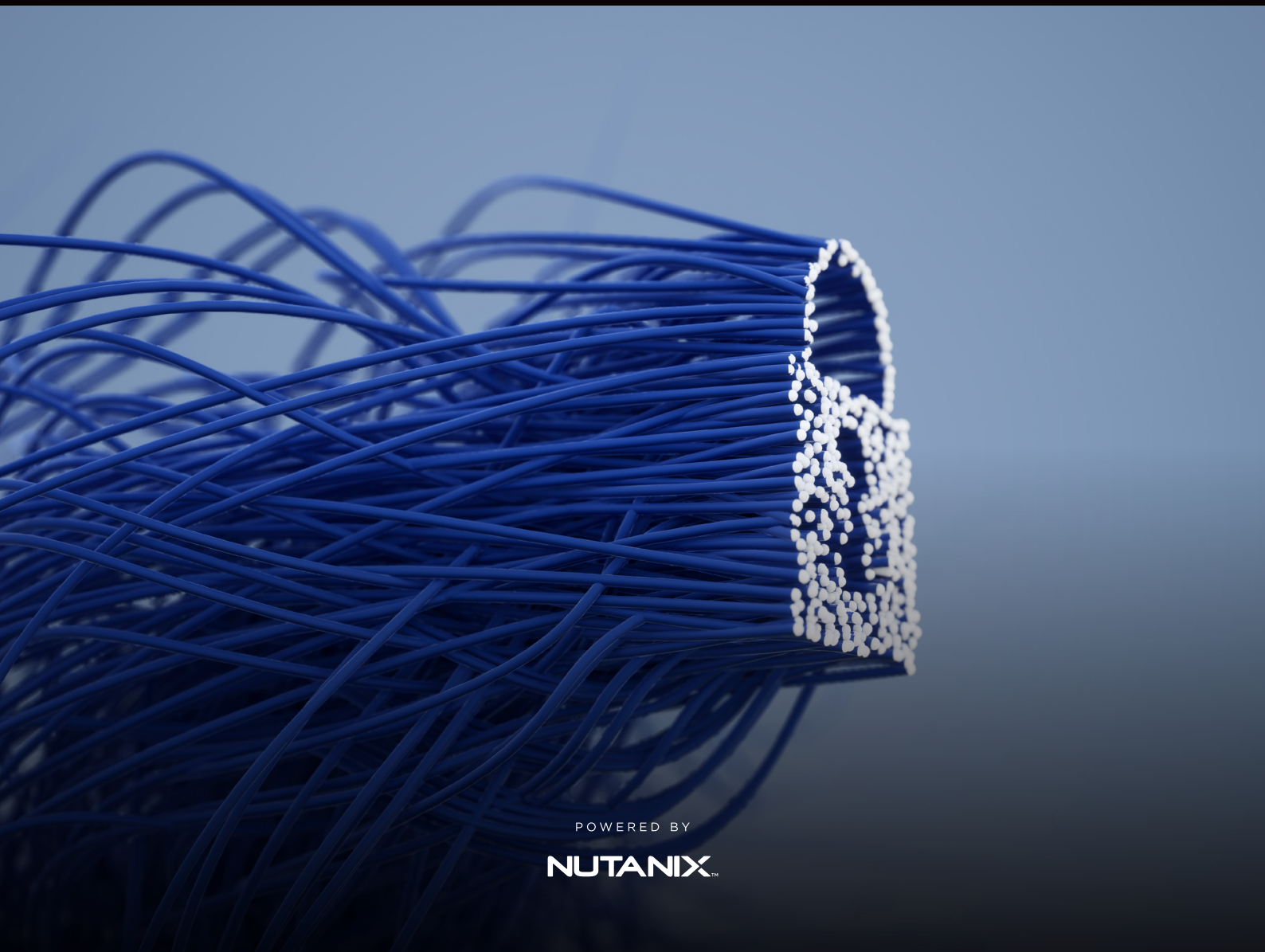
CXO FOCUS

NUTANIX MASTERCLASS SERIES: **CYBERSECURITY STRATEGY**

—

NOVEMBER 2020



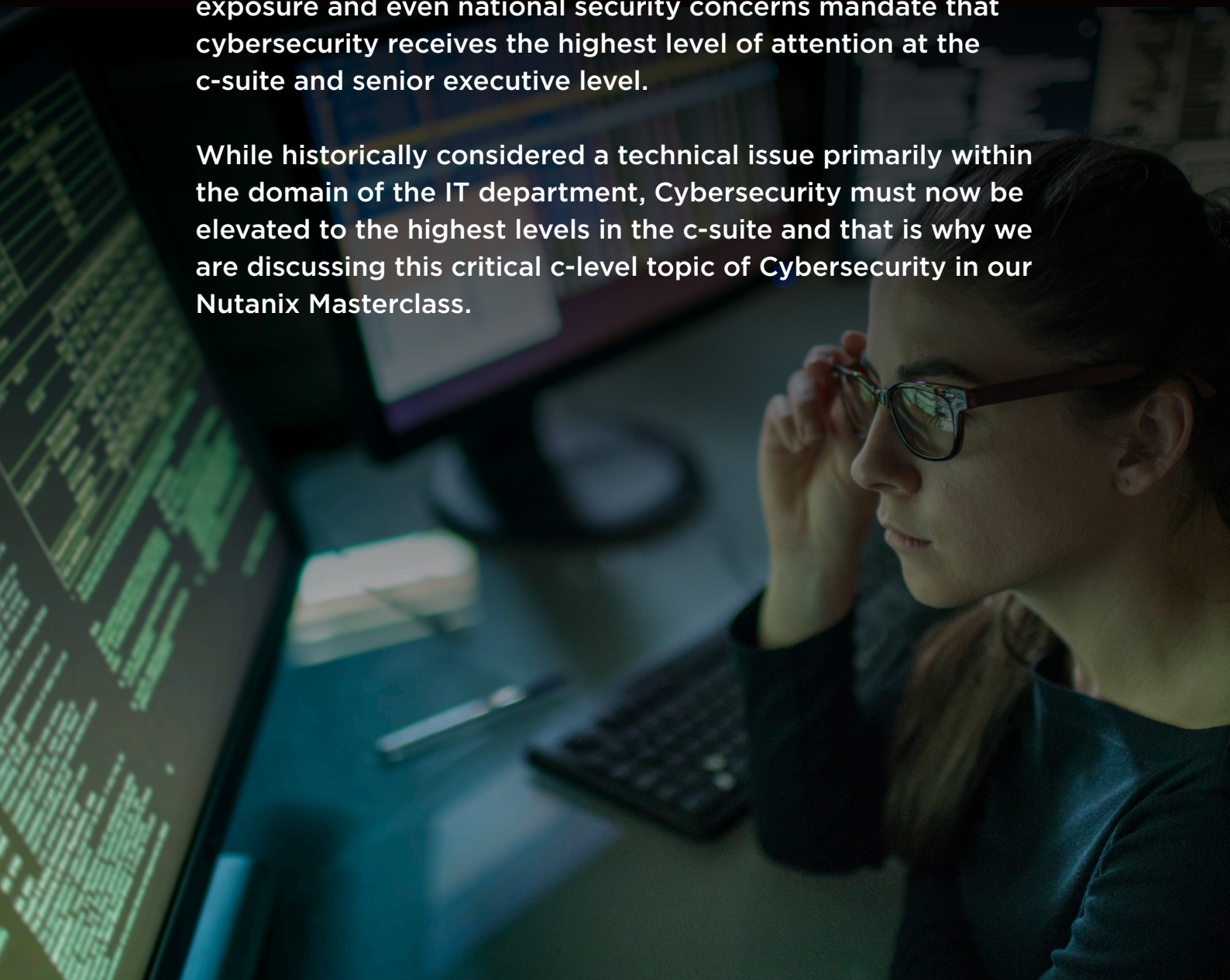
POWERED BY

NUTANIX

Cybercrime has reached pandemic proportions across the globe. In headlines every day, there are stories about cybersecurity breaches that have wreaked havoc on businesses, organizations and individuals. The global cost of cybercrime has now reached well over $600 billion, or about 0.8 percent of global GDP. No company, organization, industry, individual or country is immune to cybercrime.

And with technology advancements in Cloud, IOT, and 5G, the need for effective cybersecurity becomes even more critical. The financial losses, reputation/brand damage, legal exposure and even national security concerns mandate that cybersecurity receives the highest level of attention at the c-suite and senior executive level.

While historically considered a technical issue primarily within the domain of the IT department, Cybersecurity must now be elevated to the highest levels in the c-suite and that is why we are discussing this critical c-level topic of Cybersecurity in our Nutanix Masterclass.



Delivered by Dr Art Langer, Professor at Columbia University and Robert Duncan, CISO for Direct Line Group and Columbia University Cybersecurity Instructor , this invite-only Masterclass was hosted by Nutanix's own CXO Leader EJ Bodnar.

Dr Langer pointed to some of the newest issues impacting cybersecurity concerns. Among the key drivers, innovations and developments changing the risk attack surfaces out there are 5G, the explosion of IoT devices, the dramatic rise in data capture, the development of blockchain and the explosion of AI and ML across applications and the cloud.

As we welcome smarter smartphones with 5G, we will find that devices do become more useable. These are devices that will be able to store more data and perform more interactions.

"This will eventually push us towards a reality where laptop computers have a more limited lifecycle and the smartphone devices will become the most direct channel into enterprise systems. Voice technologies will get smarter too, because nobody wants to type out things that they can say," said Dr Langer.

Re-architecting for reality

We know that there is an explosion of mini-applications today running on an increasing amount of microservices and containers. This – along with core developments in blockchain- drives the replication of data in many instances, which is an opportunity for efficiencies but also opens the door to faster-spreading risks in some cases.

Talking about the 'tidal wave' of challenges coming to us in the immediate future, Dr Langer explained that all the new devices and increase in data will also increase the force of the dark web. With the amount of Input/Output (I/O) that will naturally now manifest itself, an inevitable explosion of risk will also face us.

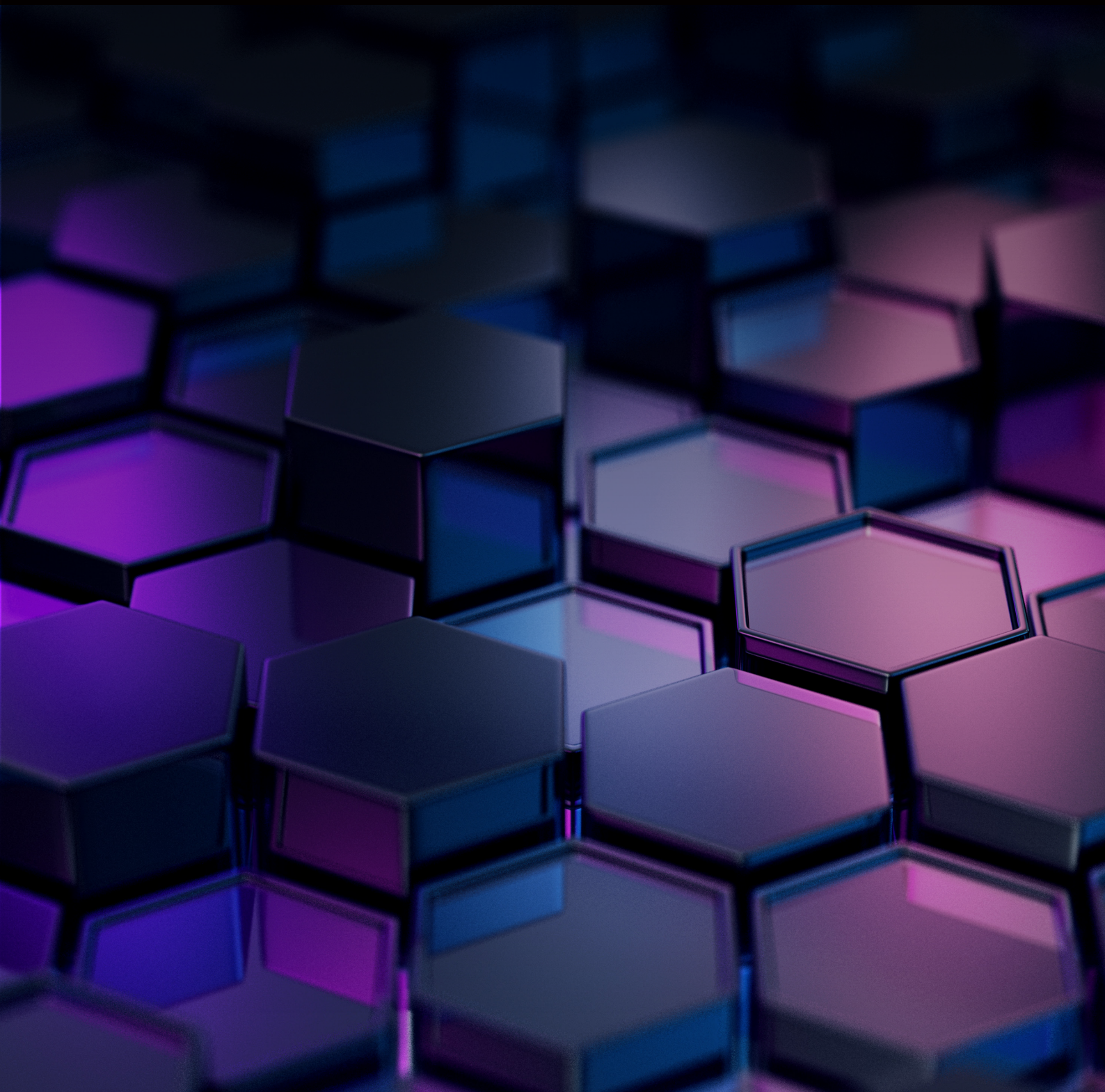
With more technology, comes more data and so comes more risk. This issue is especially problematic when we look at the legacy applications that will interface with these new wider data streams.

In so many cases, we never designed our applications with security in mind. Dr Langer thinks that the design of our systems as they are today cannot meet the challenge ahead. With blockchain-driven designs for the future, we can make some of the quantum leaps needed here. Plus, with quantum in mind, we also need to collectively decide whether quantum computing will finally deliver on the future in the way that industry evangelists think that it will.

We will move to a whole new world of platform design. Users themselves will be able to create mini-applications on their mobile devices themselves because there is a new level of independent component design working at the foundation technology substrate level.

"If you haven't thought about this at all, that is worrying. If you have started to build a strategy designed to be ready for the next new world of technology, then that is encouraging," said Dr Langer.

> If you haven't thought about this at all, that is worrying. If you have started to build a strategy designed to be ready for the next new world of technology, then that is encouraging"



Are we just chasing windmills?

Robert Duncan, CISO for Direct Line Group and Columbia University Instructor followed up on Dr Langer's thoughts.

Asking whether we can every really get to a point where we are in control of cyber-security issues, Duncan suggested that some organizations may feel like they are just 'chasing windmills' i.e. running after an endless loop that flies away. He made this comment in light of the fact that as much as companies invest in security protection layers, cyber-criminals are always constantly pushing to go one faster, one better and one level more damaging with their attacks.

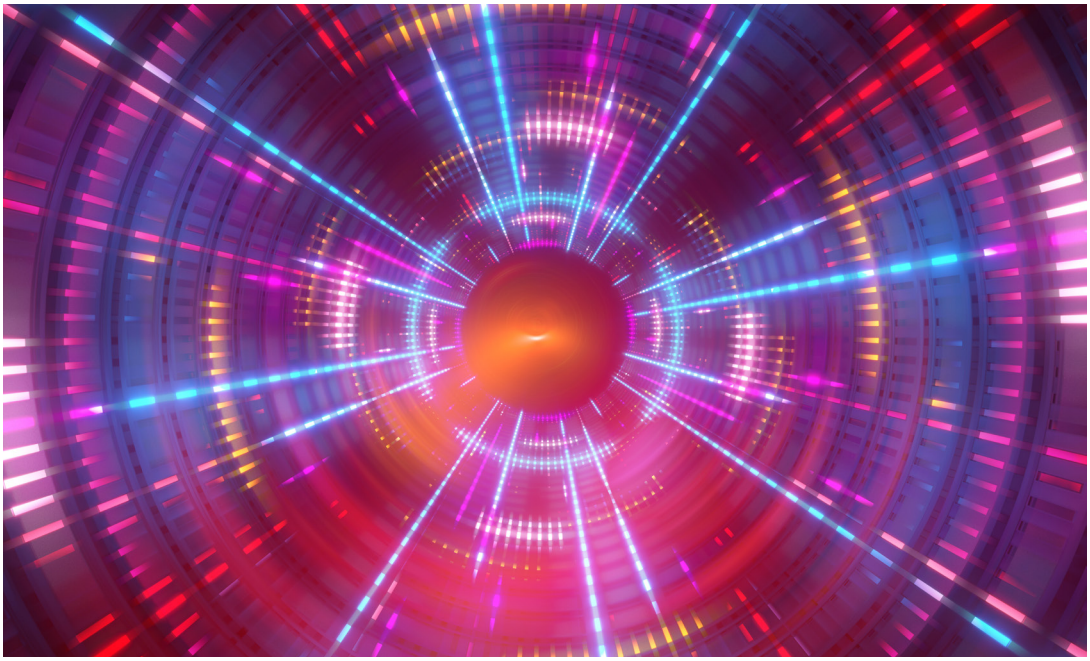
Given that many enterprises may still have legacy systems designed in the 1960s and 1970s when security really wasn't an inherent part of systems design, we need to remember that the attackers are typically using state-of-the-art equipment and techniques to target age-old technology deployments where security was 'bolted on' as an afterthought.

Pointing out why organizations worry about cyber-attacks in the first place, Duncan reminded attendees that a cyber 'event' of any kind usually has a negative impact upon the financial status and operational abilities of the company in general.

"To handle cyber-strategy competently, firms need to think about developing a comprehensive cyber-resilience strategy," said Duncan. This encompasses everything from crisis management to incident response and control. It also straddles areas including governance and security awareness, data integration and protection and areas relating to compliance from a legal and regulatory point of view.

Only when you start thinking about resilience can the organization realize that the breadth of the task involved is way more than any one single person in the role of CISO can handle. But overall, Duncan urged organizations to be resourceful and be ready to adapt... and in so doing he tabled his favorite quote that sums up this ethos. "The winning general is the one who can best act with imperfect information and half-formed theories." - Napoleon Bonaparte.

"To handle cyber-strategy competently, firms need to think about developing a comprehensive cyber-resilience strategy,"



The light at the end of the cyber-tunnel

As tough as the job of the CISO is and as far-reaching and damaging as the impact of cyber-attacks are, Duncan pointed out some areas for hope. Explaining that there is now more board-wide involvement in cyber resilience programs and initiatives, Duncan suggested that the CISO will have an increasingly engaged and involved set of other C-suite professionals to draw upon for support.

Many members of the C-suite will now want to know an organization's resilience strategy compares with that of its competitors, customers and partners. The board will now be increasing support for security by design engineering initiatives that ensure resilience are baked-in and not just bolted-on as an afterthought.

Duncan validated his points by explaining that the core responsibility of the CISO and the wider board is to examine the organization's operational base in order to work out what the 'real threats to the company' actually are i.e. in terms of the onward business impact that could be felt as the result of an attack.

There is clearly a need to get ready for the next-age of computing platforms at the lowest level and - at the same time – prepare organizations internally for the next age of business with a new strategic outlook on resilience and cyber-security as a whole. This Masterclass will help provide the roadmap for a new cybersecurity masterplan that every firm can apply.

KEEP UP TO SPEED
WITH THE LATEST CONTENT

NUTANIX.COM/CXO

POWERED BY

NUTANIX