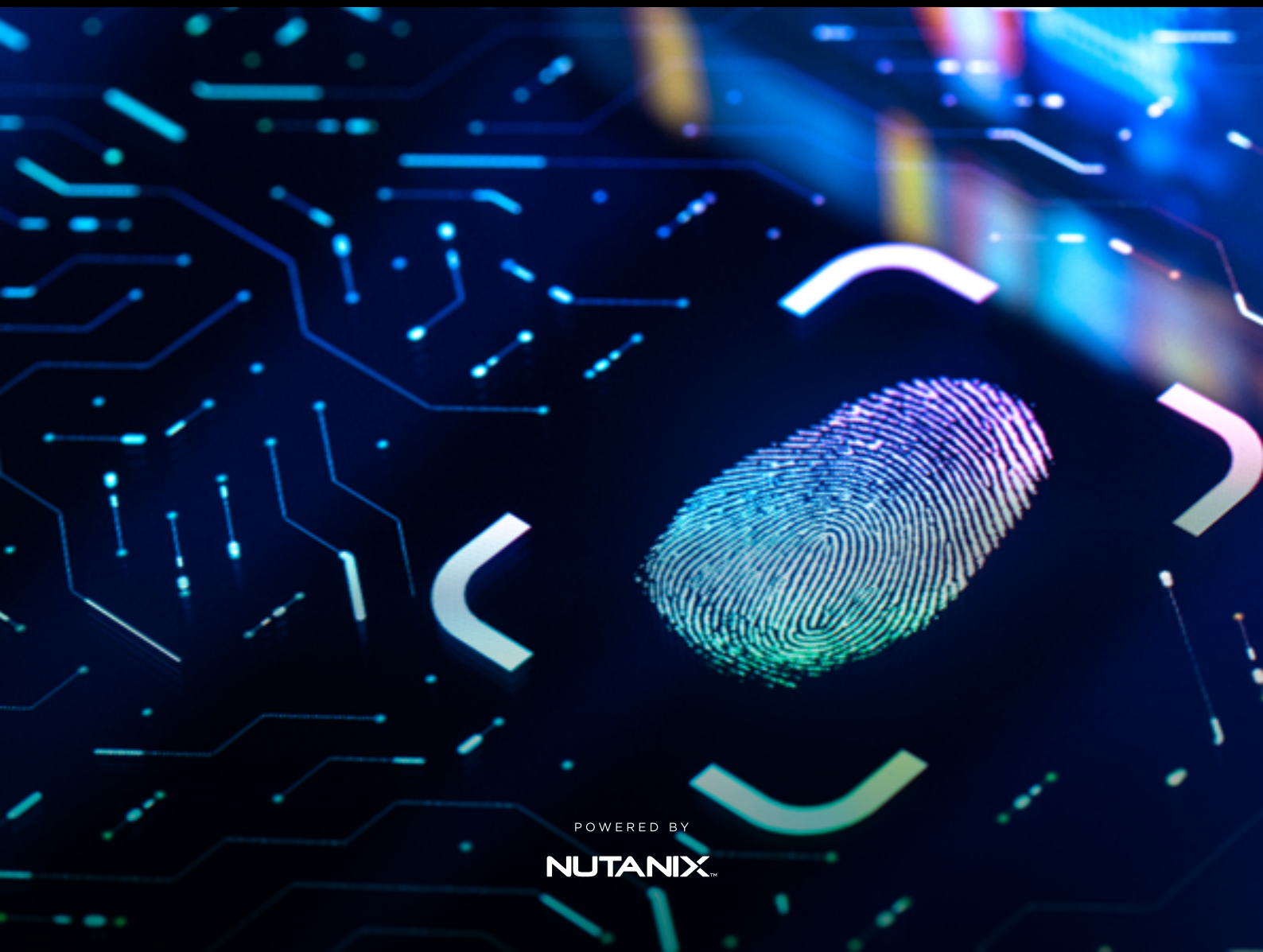
CXO FOCUS

STRONG CYBERSECURITY IMPROVES INNOVATION

AS CYBERSECURITY CONCERNS INCREASE, BUSINESS AND TECHNOLOGY LEADERS CAN RAMP UP PROTECTION AND OPPORTUNITY.

—

APRIL 2022



CXOs are walking a tightrope. There's constant pressure to enable and deliver cutting-edge technology innovation. At the same time, cyberthreats against organizations are on the rise. Walking that fine line of safeguarding your organization while being a vehicle of positive change is a tough act. But it is achievable.

According to the 2022 Global Cybersecurity Outlook report by the World Economic Forum, ransomware threats rose by 151% in 2021, resulting in about 270 attacks per organization, a 31% increase over the previous year. And each successful attack cost the victim organizations an average of $3.6 million.

The same report found that victim organizations suffered a 3% decline in market value up to six months after the attacks were publicly disclosed. Furthermore, most victim organizations required 280 days to full contain the issue.

Some 80% of surveyed business leaders told the World Economic Forum that they consider ransomware a danger and a threat to public safety, which has escalated since the Russian invasion of Ukraine.

"Russia may be exploring options for potential cyberattacks," according to recent statement issued by the White House. "The president has launched public-private action plans to shore up cybersecurity…and has directed departments and agencies to use all existing government authorities to mandate new cybersecurity and network defense measures."

Opportunity cost

Unfortunately, the very technology innovations that CXOs want to deploy are creating a more vulnerable threat landscape. Automation to reduce costs and skirt the global skills shortage, along with edge computing for increased sustainability, are opening up a wider field of threat opportunities.

"By 2025, next-generation technology has the potential to overwhelm the defenses of the global security community," states the Internet of Things (IoT) Services Global Market report. "The approach to cybersecurity needs to be overhauled before the industry finds itself in any fit state to tackle the threat."

As CXOs look to next-generation technologies to counter the skills shortage, the PSA Certified 2022 Security Report cautions that a continued lack of security expertise has the potential to leave vulnerabilities unchecked.

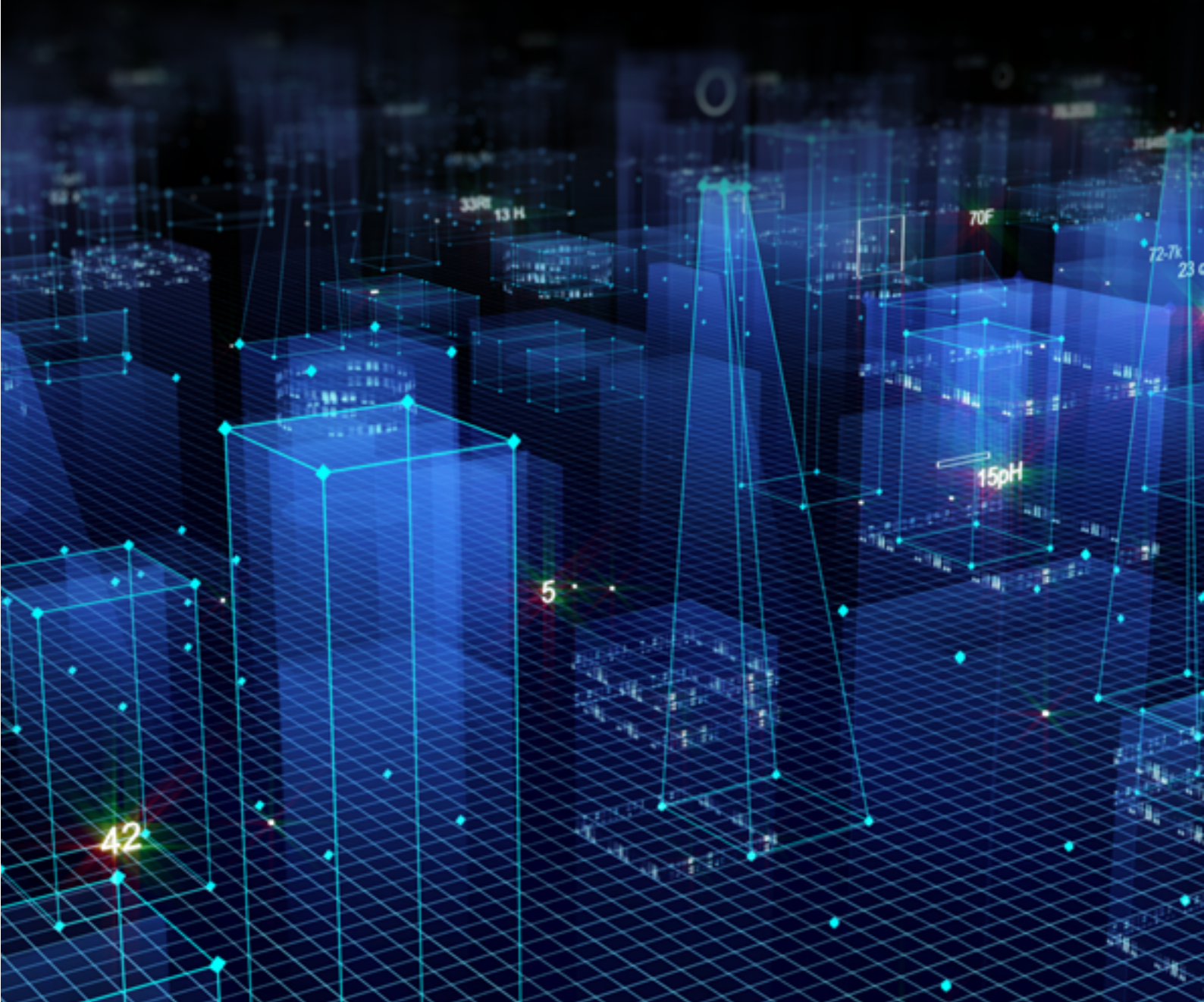
"We have to methodically assess the risks and the number of touchpoints," said Mat Mallett, chief digital information officer for the UK Space Agency, a public sector agency responsible for the satellite and rockets industry. "We have to be pragmatic and make sure that everything is commercially protected, and that the data is compliant with the General Data Protection Regulation."

However, CXOs cannot ignore the new wave of technologies or consider them with fear.

"In February last year, we were attacked by hackers because of our obsolescence," said Sylvain Coquio, group CIO for Manutan, a French-based office and school equipment supplier with operations across Europe.

Manutan partnered with enterprise cloud computing leader Nutanix to build a secure and automated platform to support its modern applications-based e-commerce website and infrastructure, which uses a hybrid cloud model. "We had to think differently, and we had to prepare for agility and digital transformation," Coquio noted.

> Security is one of the most important elements of cloud architecture... Confidentiality and integrity are vital, and we need to be able to reassure the business that we can protect client data. It's our fiduciary responsibility to always protect their data.



Security as architecture

In the past, security was often treated as an afterthought, long after the deployment of a technology or business strategy. Today CXOs closely examine and consider cybersecurity requirements at the start of every planning process that involves enterprise architecture.

"Security is one of the most important elements of cloud architecture," said Mudassar Ulhaq, CIO of financial services organization Waverton. "Confidentiality and integrity are vital, and we need to be able to reassure the business that we can protect client data. It's our fiduciary responsibility to always protect their data."

Ulhaq has led a major enterprise cloud computing adoption effort at Waverton. The CIO noted that the close integration between applications and the built-in defenses of Microsoft Azure has improved the security posture of Waverton. The CIO is also on the risk management committee for bankers.

"Architect your services to continuously use specific clouds for particular tasks, such as the public cloud for scalability and elasticity and the private cloud for predictability and security," said Nutanix CIO Wendy M. Pfeiffer.

With cybersecurity architected into the technology foundations of the organization, CXOs are finding that this allows them to focus on creating a resilient business. And if an organization has a culture that is resilient, the impact of a cyberattack can be dealt with swiftly and efficiently, fully restoring business operations.

"Organizations need to work more closely with ecosystem partners and other third parties to make cybersecurity part of an organization's DNA and to be resilient and promote customer trust," said Accenture CEO Julie Sweet.

Jeremy Jurgens of the World Economic Forum agrees, saying that "Companies must now embrace cyber resilience – not only defending against cyberattacks but also preparing for swift and timely incident response and recovery when an attack does occur."

This is the surest path to improve confidence in resiliency across an enterprise organization. Despite this, the World Economic Forum finds that less than one-fifth of business leaders are confident that their organization can be resilient in the face of a cyberattack.

"We are at a crossroads where cyber resilience has become the defining mandate of our time – beyond foundational security controls – to anticipate future threats, withstand, recover from cyberattacks, and adapt to likely future digital shocks," said Algirde Pipikaite, cybersecurity strategy lead at the World Economic Forum.

A resilient organization also has the strength to continually innovate. Being able to identify threats is a skill equal to that of spotting opportunities. As a CXO, there will be blustery days when you must walk a tightrope. But when you're able to detect, respond and mitigate threats early, it means you've seized the opportunity and reached the other side.

KEEP UP TO SPEED
WITH THE LATEST CONTENT

NUTANIX.COM/CXO

POWERED BY

NUTANIX