



CXO FOCUS

# CISOs MUST BECOME STRATEGIC BUSINESS LEADERS

NEW TECHNOLOGIES AND THREATS REQUIRE BUSINESS AND TECHNOLOGICAL EXPERTISE




SEPTEMBER 2022



POWERED BY  
**NUTANIX**<sup>™</sup>





## Technology is changing at a rapid pace. The role of the Chief Information Security Officer (CISO), therefore, has to change.

A rising level of complexity as a result of new technologies means that CISOs and Chief Information Officers (CIO) need to become increasingly strategic, and therefore, business leaders that do more than just protect the organization but also develop a culture and methodology to deal with the rising level of cybersecurity threats.

A wave of new technologies will increase the security challenge for organizations, as executive boards and customers expect the organization to adapt and adopt these technologies. Dr. Art Langer, Vice Chair of Faculty and Executive Advisor to the Dean at Columbia University, believes the roll-out of 5G networking will be a significant cybersecurity challenge. “It is 100 times faster than 4G. 5G will allow us

to move data back and forth between smartphones and internet of things (IoT) devices, and this means there will be a tremendous increase in IoT devices.” But the Director of the Center for Technology Management believes this is just the beginning of a series of disruptive technologies about to enter the enterprise. He believes Blockchain type technologies will become more prevalent, and that the silicon chip that has been the foundation of the last 50 years of technology innovation will be replaced by quantum and DNA chips. To cope with existing and near-term demands for digitization, Langer says CIOs and CISOs will need to: “move to platform designs like those used by the digital companies, such as Amazon. There will be an explosion of mini-applications that drive the replication of data,” he says.



“All of this will increase the move to the cloud, and it is the end of the relational database model,” Dr. Langer says.

With the current scale of threat estimated to be valued at \$600 billion of gross domestic product (GDP), organizations and their business technology leaders face an increasing threat level. “Boards worry about the reputational damage of a big breach, Equifax being a classic example where you could see the correlation between the attack and the stock price,” says CISO Robert Duncan of Ardagh Group, a supplier of packaging.

Duncan, who is also a Columbia faculty member, says organizations have become aware and better informed of the risks of poor cybersecurity. “In 2015, the CEO of mobile operator Talk Talk, Dido Harding, revealed that the

company had lost data in a breach, but did not know how much data had been lost.” Harding and the response of Talk Talk became shorthand, in the UK at least, for poor leadership and how not to deal with a breach. “That spooked a lot of CEOs, CIOs, and CISOs. It is not just about protecting your company; it is what you do when something happens,” Duncan says of how the CISO and the entire leadership team need to be strategic in response to a breach.

“Most of the security we enjoy today is the concept of the perimeter, keep the bad people from getting in. But, once you pierce that line, then your applications and data tend not to be very well protected,” says Dr. Langer of the weakness in many organizations’ cybersecurity practices. “The perimeter concept doesn’t work, so we need a new type of process.”





## It's getting complex

Although digital business methods simplify the organization, the truth of modern global business is that it is complex. That complexity makes the role of delivering resilient cybersecurity tough for CISOs and CIOs.

Duncan says this situation is a continuum: “Up to the 1970s, the main devices that people interacted with were the radio, television, and the car.

In the 1990s, things got really interesting with the PC and then the e-commerce and dot com boom leading towards the smartphone and now IoT.”

“If you think of the world that a CISO has to defend, it is dramatically difficult. Today an attacker can initiate an attack for a small amount of money,” he says.

If you think of the world that a CISO has to defend, it is dramatically difficult. Today an attacker can initiate an attack for a small amount of money.



## Time to be strategic

**A**s organizations become more complex, digital, and under increasing cybersecurity threat, the role of the CISO must change. “It is not enough for the CISO or CIO to be focussed on security,” Duncan says. He describes the CISO role as a curious job title, which encompasses architecture, people management, and technology operations. At a Fortune 500 or FTSE 100 business, Duncan says the CISO should be responsible for crisis management, data privacy, holistic security as well as cybersecurity. “There is no perfect model; it depends on the relationship between the individuals,” he says of how CISOs and CIOs should work together in an enterprise.

“Executive involvement has improved dramatically over the last seven years,” Duncan says of how CISOs are benefitting from the increased awareness of cybersecurity following

the Talk Talk, Equifax, and Marriott Hotels breaches. This means that CISOs are spending more time with the executive leadership of the organization, which has its own challenges. “The board will bring questions such as ‘am I paying enough? What is a good metric for the cybersecurity budget? How many times have we been attacked? How many times have we lost data?’

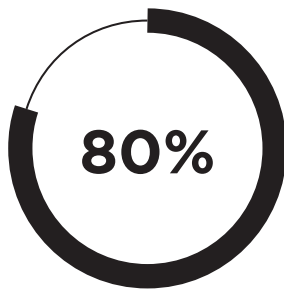
“So you have to work with your executive team on these questions and take them on a journey to think about the risks and probabilities,” Duncan advises. Dr. Langer adds that the CISO must take part in regular interactions with the board and says to CISOs: “You have to do all the security that you are doing now and redefine the role in terms of providing strategic advice.” Langer says the CISO role is evolving to include cultural change and executive leadership.



“When you talk to the board, it has to be something you do regularly, and you will already have had conversations with them,” he says of ensuring board members are aware of the challenges you face and what plans as CISO you have to deal with them. Dr. Langer says at the board CISOs must not be shy of revealing how good they and their team are, how they deal with third-party suppliers, and being able to compare the cybersecurity posture of the organization to its rivals. “CISOs need to move beyond being a supportive organization. If you have influence, you have leadership.”

With marketing and communications to the business, and in the event of a breach to the

customer base involved, the modern strategic CISO cannot just be technically brilliant. Not only must today’s strategic CISO take the executive leadership on a journey, but Duncan also says often, the cybersecurity team needs to be helped too. He says cybersecurity teams can be reactionary; they say no, use jargon, and are often junior or under-invested in. Just as the CISO’s role is becoming more strategic, so too must the cybersecurity team become more business-friendly and aware of the wider challenges and opportunities the business faces. “CISOs spend 80% of their time in the field. CISOs must do that, and you have to get people beneath you to do the day-to-day,” Dr. Langer adds.



CIOs spend 80% of their time in the field. CISOs must do that, and you have to get people beneath you to do the day-to-day





A strategic CISO and cybersecurity team will be able to ensure an organization is resilient. “Building a cyber resilient model is quite different to a typical cybersecurity mandate,” Duncan says. A cyber resilient organization has to be ready for what Duncan describes as the respond and recover phase and is, therefore, an organization that is aware that an attack or breach is highly probable. The team will not then just place its efforts into defense and protection but dealing with the inevitable.

Cybersecurity is high on the leadership agenda, in part, due to a number of new regulations which place responsibility on the executive board, as well as a price on failure.

Duncan says new legislation has helped but has also added further headaches to the CISO role. Complying with regulations can, the CISO says, build the perception of security, which is not the same as being a cyber resilient organization. “Regulations are important because you have to show that you have thought about what is going to happen, and at the very least, you have a good paper trail. So a regulator like the Information Commissioner’s Office (ICO) in the UK can see that you have a good recovery plan in place, and the fine may be lower.”

Duncan says strategic CISOs need to: “think about a real-time risk appetite”. “You can then bring the company into the security design and the development of the culture.”



Regulations are important because you have to show that you have thought about what is going to happen, and at the very least, you have a good paper trail.”







The global cybersecurity market was valued at \$184.9 billion, according to market researchers Grand View Research, who expect the industry to grow at an annual compound rate of 12% from 2022 to 2030



Cybersecurity technology is big business; in 2021, the global cybersecurity market was valued at \$184.9 billion, according to market researchers Grand View Research, who expect the industry to grow at an annual compound rate of 12% from 2022 to 2030. CISO Duncan warns security and business technology leaders about introducing too much technology into the cybersecurity program. “There are a lot of tools out there. Threat maps are interesting to look at if you are not technical, but they don’t tell you anything about your own company. Threat intelligence is great to have as it gives you insight into the activity on the dark web, for example. So be careful, introduce tooling that leads to clear, tangible results.”

A tool Duncan says is very valuable to strategic CISOs is the kill chain. “It is a nice way to show how an attack really happens.”

But tools are only part of the story; Duncan uses the analogy of the Maginot Line, a physical and fortified line built in France following World War I. The line has become a byword for failed security as by 1939 and the rise of Fascism, the Nazi forces went around the line and invaded France from a different direction. However, as Duncan points out, the architect of the Maginot Line, André Maginot, proposed not only the line of fortresses but also a rapid reaction force that would be able to respond to a different type of attack. Having invested in and built the Maginot Line, the French government didn’t approve the rapid reaction force, and, as they say, the rest is history.



“That happens all the time in the enterprise as there is not an investment in security awareness,” Duncan says of board-level backing for new technology, but not change management. “Two people on \$40 to \$50,000 to run security awareness around your company would make a big difference, but there is an understanding that it’s just like marketing. The technology is the easy part; the push back is the people and process part.”

As well as tools, frameworks can help organizations develop cybersecurity resilience. “NIST is a great framework to explain to executives what is required,” Duncan says of the National Institute of Standards and Technology (NIST) cybersecurity framework developed by the US Department of Commerce. Whilst continuous testing by

red teams is vital. “Think about the threat actors, what they might do and how and what you need to do in response. Then think about the risk in terms of primary and secondary loss. This means impacts are understood by interested parties,” Duncan says of how to explain what a breach means to the business, its P&L, and services.

“If you don’t have a security culture, it is impossible to be an effective CISO. The attitude towards security by the executive team and your employees is vital,” Duncan says. The CISO describes cybersecurity strategy as being like the classic iceberg. “Above the waterline is all the things that you can see, like your policies and standards.” Below the waterline is where both the danger and the real power lie.



It is for this reason that CISO Duncan advises organizations have a playbook, similar to the run books that airline pilots have as a guide of steps to dealing with a dangerous scenario on a flight. The playbook will direct all actions in the event of an cyber attack. “The playbook helps you consider the communications, restoring systems, who is in the chair, how you manage uncertainty and delegated responsibilities,” Duncan says.

Technology is changing at a rapid pace, and for organizations to become cyber resilient, the role of the CISO has to become strategic and business oriented. Strategic cybersecurity requires business leadership by leaders that do more than just protect the organization, but also develop a culture and methodology to deal with the rising level of cybersecurity threats.



The playbook helps you consider the communications, restoring systems, who is in the chair, how you manage uncertainty and delegated responsibilities”





KEEP UP TO SPEED  
WITH THE LATEST CONTENT

[NUTANIX.COM/CXO](https://www.nutanix.com/cxo)

POWERED BY

**NUTANIX**<sup>™</sup>