CYBERSECURITY

These will be the main cybersecurity trends in 2020

Jan 7, 2020

Dorit Dor
Chief Technology Officer, Check Point Software Technologies

This article is part of:
World Economic Forum Annual Meeting

- **The east-west 'cyber cold war' is set to intensify**
- **5G and the IoT could make us all more vulnerable to cyberattack**
- **Businesses will start to rethink their approach to the cloud**

The world is more connected than ever. We are becoming more technologically advanced, markets are stronger, and central technologies that encompass our daily actions are constantly emerging.

These technological advances are based on seamless connectivity. As our digital transformation continues, we continue to build a more cohesive and connected society. Our data is now shared and used by more platforms than ever – in the datacentre, on the cloud and event on internet of things (IoT) devices, for example - and this trend will only increase. But this huge benefit comes with a cost. The more connected we become, the more vulnerable our data is.

Have you read?

- **Hardware is a cybersecurity risk. Here's what we need to know**
- **Cities are easy prey for cybercriminals. Here's how they can fight back**
- **5G will change the world - but who will keep it safe?**

Forewarned is forearmed. These are what I believe will be the main trends of cybersecurity in 2020:

1) The 'cyber cold war' intensifies

A new cyber 'cold war' is taking place online as Western and Eastern powers increasingly separate their technologies and intelligence. The ongoing trade feud between the US and China, and the decoupling of these two huge economies, is a clear sign. Cyberattacks will increasingly be used as proxy conflicts between smaller countries, funded and enabled by larger nations looking to consolidate and extend their respective spheres of influence.

Furthermore, utilities and critical infrastructures continue to be a target of cyberattacks, as seen in attacks on US and South African utility companies this year. Nations will need to consider dramatically strengthening cyber defenses around their critical infrastructure.

DISCOVER

How is the Forum tackling global cybersecurity challenges?

The World Economic Forum's Centre for Cybersecurity at the forefront of addressing global cybersecurity challenges and making the digital world safer for everyone.

Our goal is to enable secure and resilient digital and technological advancements for both individuals and organizations. As an independent and impartial platform, the Centre brings together a diverse range of experts from public and private sectors. We focus on elevating cybersecurity as a key strategic priority and drive collaborative initiatives worldwide to respond effectively to the most pressing security threats in the digital realm.

Learn more about our impact:

- **Cyber resilience:** Working with more than 170 partners, our centre is playing a pivotal role in enhancing cyber resilience across multiple industries: oil and gas, electricity, manufacturing and aviation.

Want to know more about our centre's impact or get involved? Contact us.

2) The rise of artificial intelligence (AI)

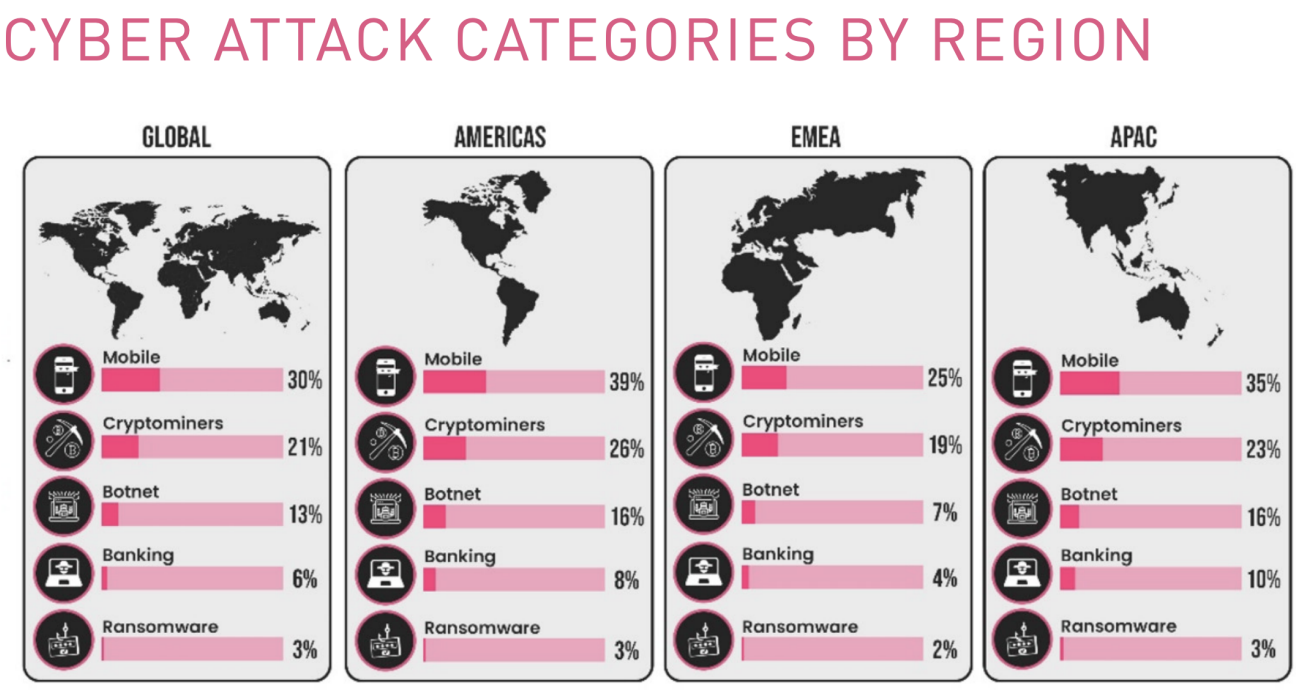
The US elections in 2016 saw the beginning of AI-based propagation of fake news. Political campaigns devoted resources to creating special teams that orchestrated and spread false stories to undermine their opponents. As we prepare for major elections worldwide in 2020, we can expect to see these activities in full effect once again.

As AI continues to be used as a proxy for crime, it will also be used to accelerate security responses. Most security solutions are based on detection engines built on human-made logic, but keeping this up-to-date against the latest threats and across new technologies and devices is impossible to do manually. AI dramatically

starting to take advantage of the same techniques to help them probe networks, find vulnerabilities and develop more evasive malware.

3) Our means of communication will become more weaponized

The notion that connectivity creates new combat landscapes is proven by the developing spheres of today's and tomorrow's cyberattacks. In the first half of 2019 we saw a 50% increase in mobile banking malware compared with last year, which means that our payment data, credentials and funds are handed over to cyberattackers in the innocent click of a button on our mobile devices. The attempts of cybercriminals to trick consumers to hand out their personal data through their most common means of communications will intensify and will range from email to SMS texting attacks, social media posts and gaming platforms. Whatever we use most frequently can become a more popular attack surface.



Cyberattack trends by region in 2019 Image: Check Point

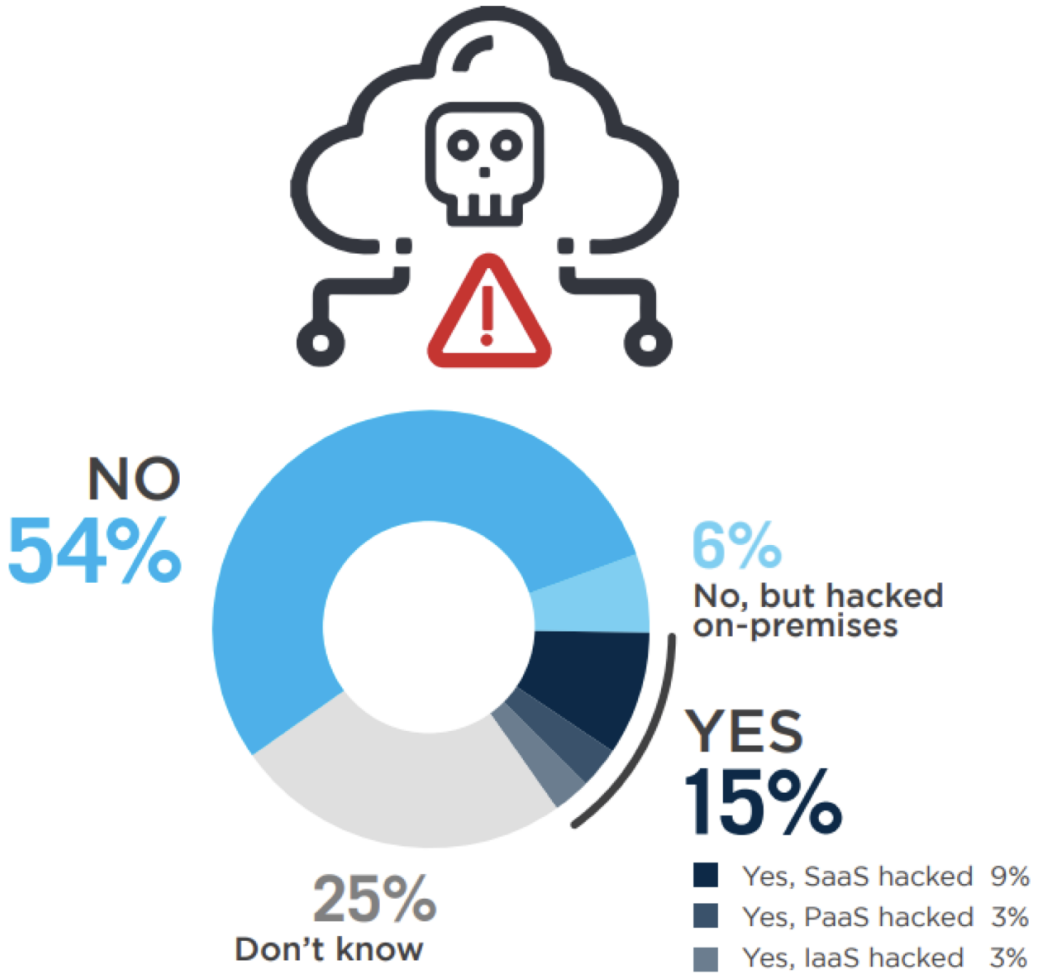
4) 5G development and adoption of IoT devices increase vulnerability

vector 5th generation cyberattacks. IoT devices and their connections to networks and clouds are still a weak link in security. This ever-growing volume of personal data will need securing against breaches and theft. We need a more holistic approach to IoT security, combining traditional and new controls to protect these ever-growing networks across all industry and business sectors.

5) Enterprises will rethink their cloud approach

Detection is no longer enough to ensure protection, and prevention is now the key to being secure.

Organizations already run a majority of their workloads in the cloud, but the level of understanding about security in the cloud remains low; in fact it is often an afterthought in cloud deployments. Security solutions need to evolve to new, flexible, cloud-based architectures that deliver scalable protection at speed.



Time for a rethink? Image: Check Point

Looking forward

Hardly a day goes by without a breach or cyber incident being reported. Attacks have become so damaging that the FBI has softened its stance on paying ransoms: the agency now acknowledges that in some cases, businesses may need to consider paying to protect shareholders, employees and customers. Through our ThreatCloud share intelligence technology we saw nearly 90 billion compromise attempts per day – compared with an estimated 6 billion daily searches on Google. These are new records which constantly being broken as time goes on, which means that the scope of victims is getting broader.

will force all of us to think about how to consolidate. In 2020 more than ever, cyberattacks are no longer a question of if, but of how and when. This is a concern that applies to us all.

Stay up to date:

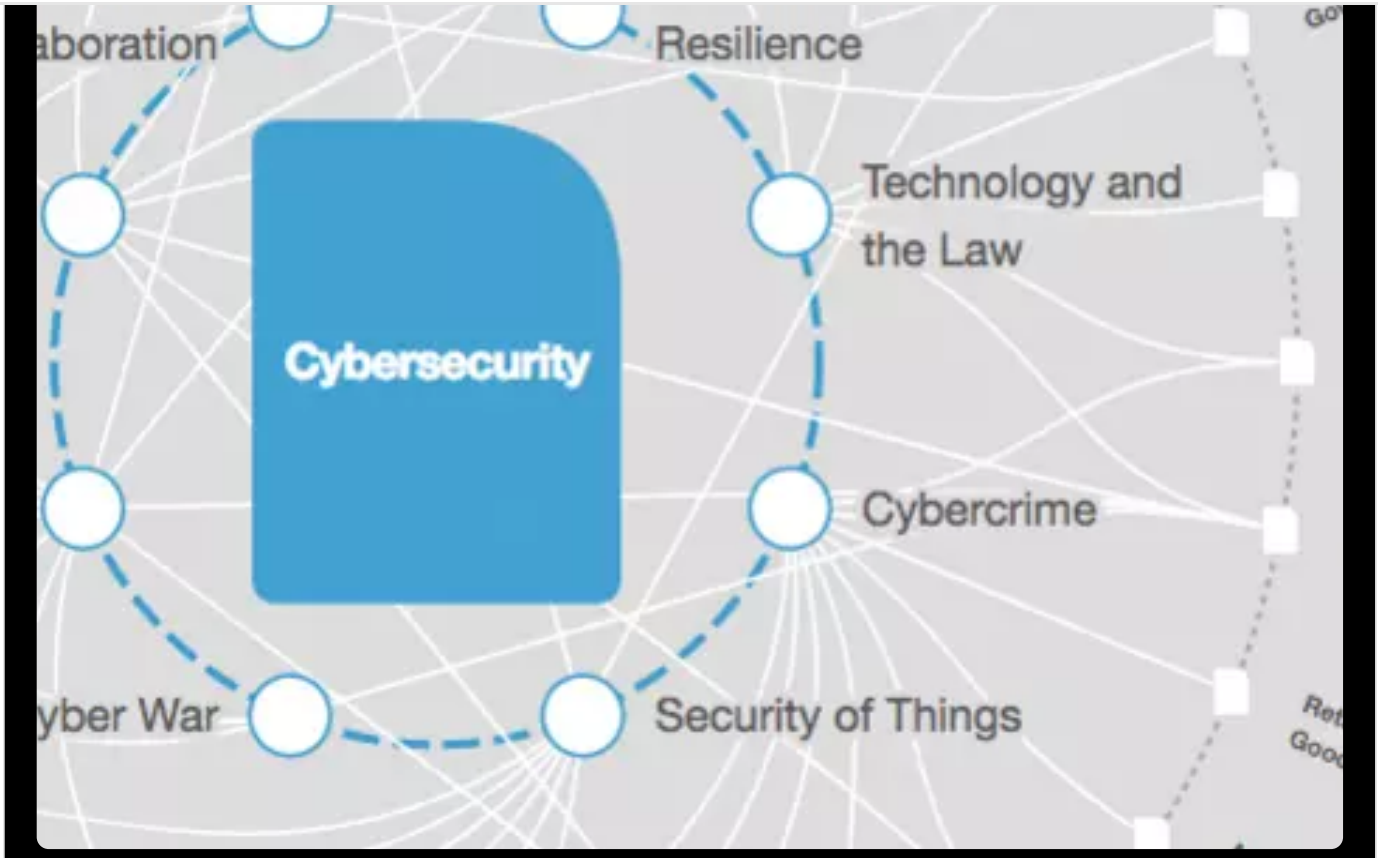
Cybersecurity

Follow

Related topics:

Cybersecurity | Davos Agenda | Fourth Industrial Revolution

Share:



THE BIG PICTURE

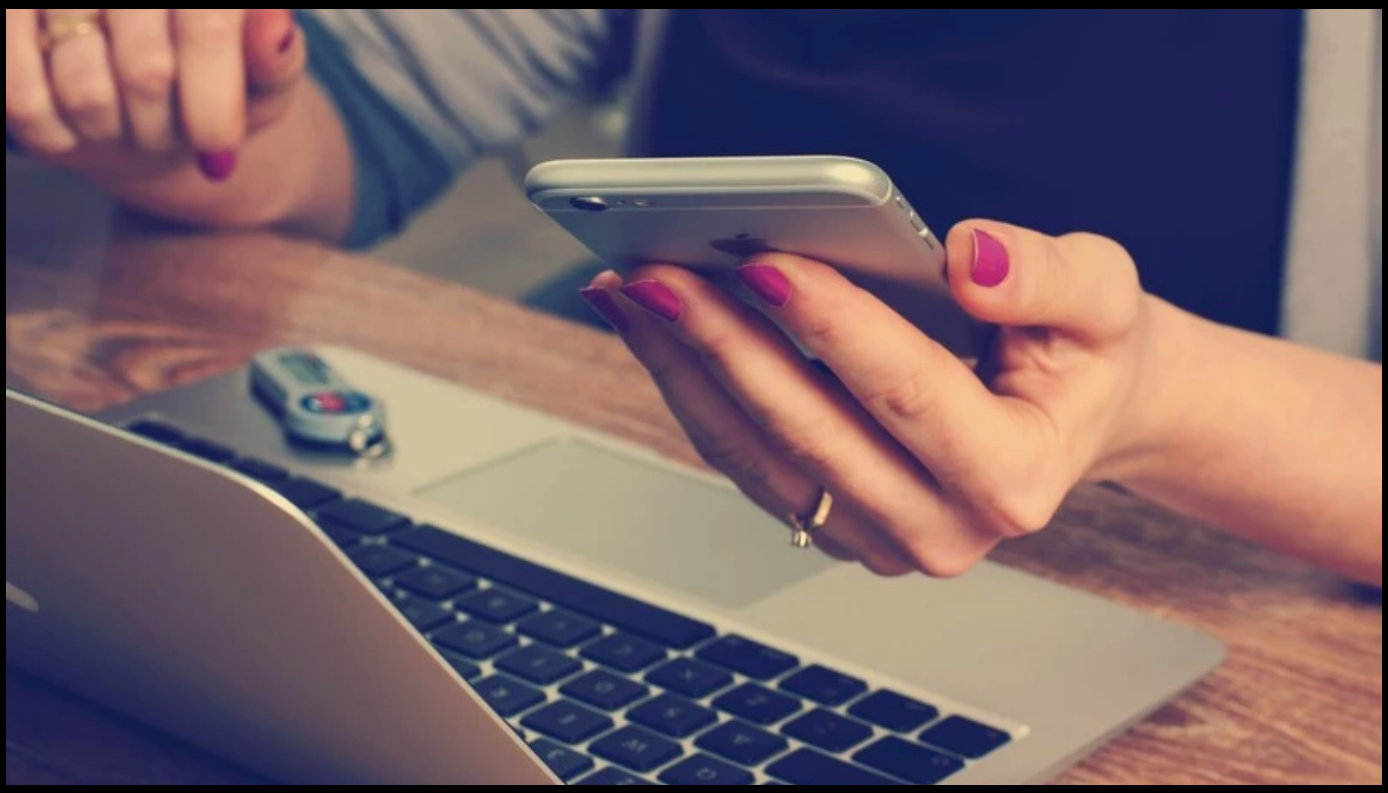
Explore and monitor how Cybersecurity is affecting economies, industries and global issues

Strategic
Intelligence

CROWDSOURCE INNOVATION

Get involved with our crowdsourced digital platform to deliver impact at scale

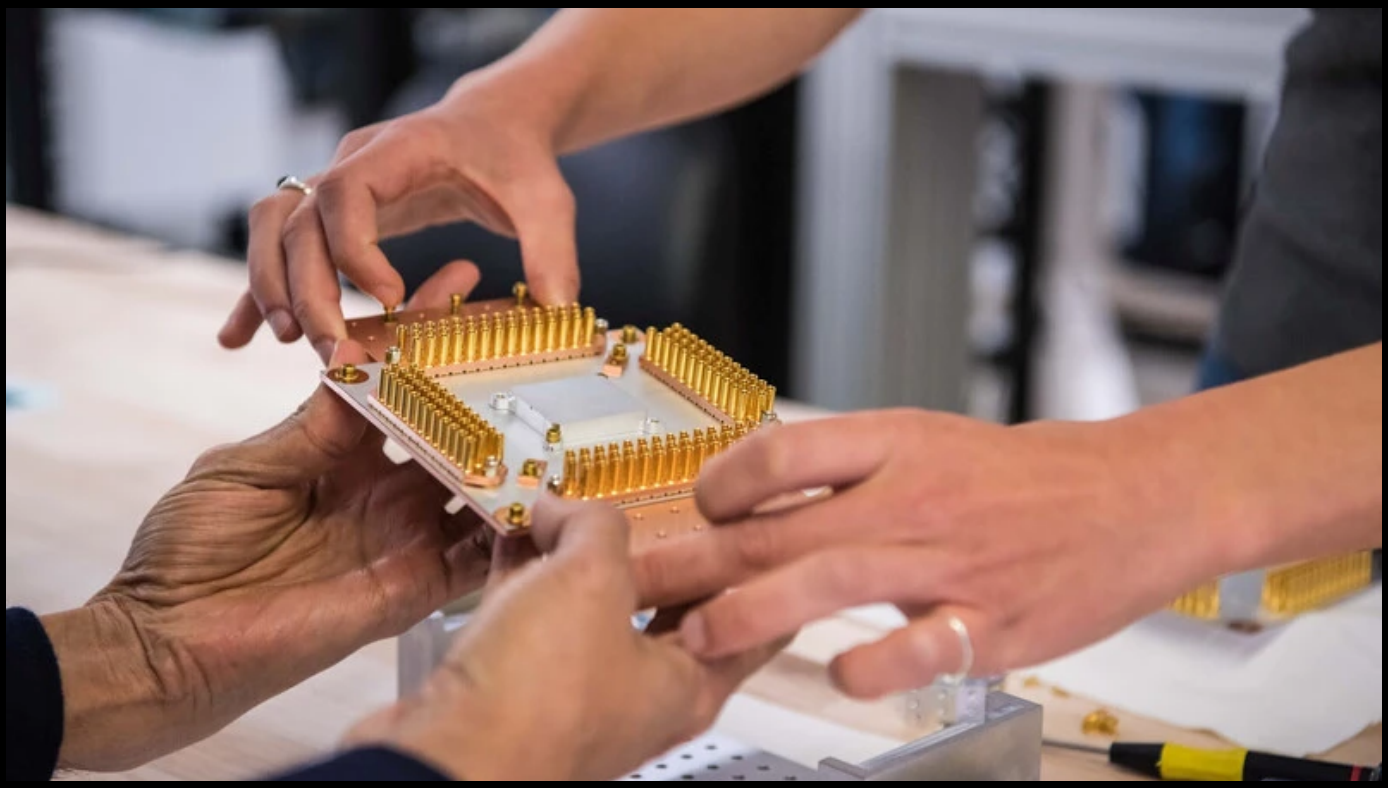
uplink



Digital safety is at a crossroads – here's how we navigate online threats globally

Agustina Callegari

February 7, 2024



Can we build a safe and inclusive 'quantum economy'?

Victoria Masterson

Healthcare pays the highest price of any sector for cyberattacks — that's why cyber resilience is key

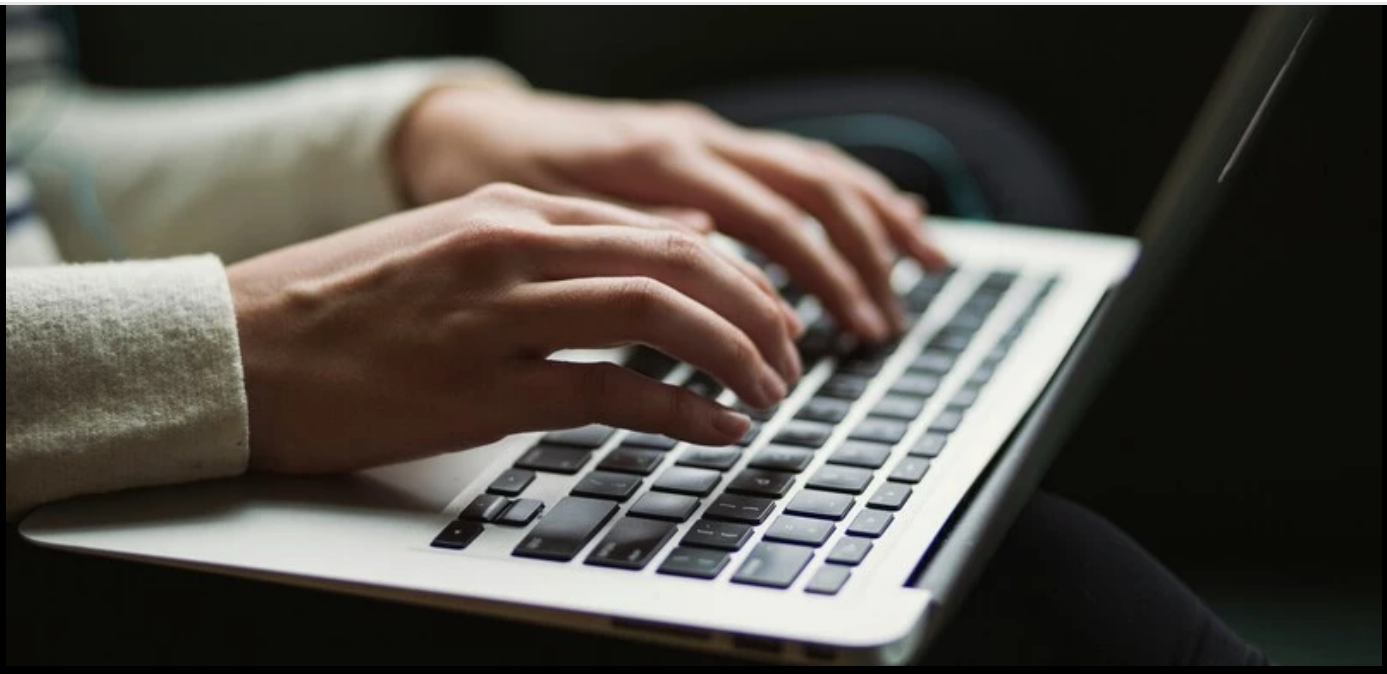
Kesang Tashi Ukyab and Filipe Beato

February 1, 2024

How advanced manufacturing can improve supply chain resilience and cybersecurity

Maya Ben Dror

January 31, 2024



AI will make bogus emails appear genuine, and other cybersecurity news to know this month

Akshay Joshi

January 29, 2024

Reflections on Davos 2024: The state of cybersecurity

Akshay Joshi

January 25, 2024

ABOUT US

Our Mission

Our Impact

Leadership and Governance

Partners

Sustainability at the Forum

History

Careers

Contact Us

EVENTS

Events

Open Forum

MEDIA

Press

Subscribe to our press releases

Pictures

MORE FROM THE FORUM

Strategic Intelligence

UpLink

Global Shapers

Young Global Leaders

Schwab Foundation for Social Entrepreneurship