CYBERSECURITY

# These are the top cybersecurity challenges of 2021

Jan 21, 2021


The latest in a long line of cyber attacks.
Image: REUTERS/Sergio Flores

**Algirde Pipikaite**
**Lead, Strategic Initiatives,** World Economic Forum

**Marc Barrachin**
**Managing Director, Product Research and Innovation,** S&P Global

**Scott Crawford**
**Information Security Research Head, 451 Research,** S&P Global Market Intelligence

- **Corporate leaders are increasingly elevating the importance of cybersecurity to their companies.**
- **But recent high-profile attacks show how much more needs to be done in the year ahead.**
- **Here are the five biggest cybersecurity challenges that must be overcome.**

---

The far-reaching cybersecurity breaches of 2020, culminating in the widespread Solarwinds supply chain attack, were a reminder to decision-makers around the world of the heightened importance of cybersecurity. Cybersecurity is a board-level issue now for many firms.

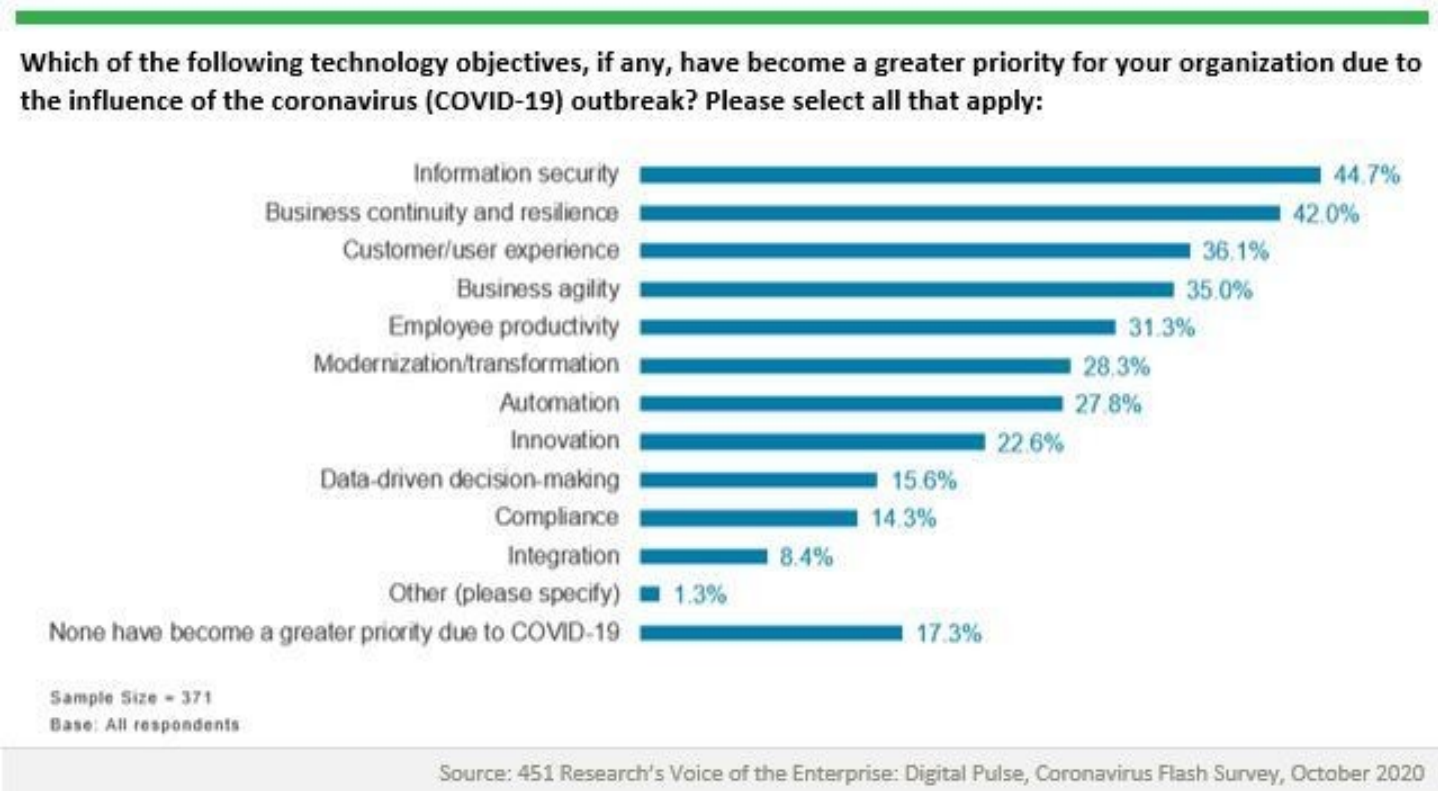



Image: Per S&P Global's 451 Research Voice of the Enterprise: Digital Pulse October 2020 Coronavirus Flash Survey, information security was the priority most often cited by respondents as having become greater due to COVID-19:

---

same time exacerbated the tech inequalities within and between societies.

Looking at the year ahead, it is critical to continue elevating cybersecurity as a strategic business issue and develop more partnerships between industries, business leaders, regulators and policymakers. Just like any other strategic societal challenge, cybersecurity cannot be addressed in silos.

Here is a list of five main cybersecurity challenges that global leaders should consider and tackle in 2021.

**Have you read?**

- **What would a cyberwar look like?**
- **We need to rethink cybersecurity for a post-pandemic world. Here's how**
- **How used-cars sales explain the cybersecurity market - and how we can fix it**

---

### 1. More complex cybersecurity challenges

Digitalization increasingly impacts all aspects of our lives and industries. We are seeing the rapid adoption of machine learning and artificial intelligence tools, as well as an increasing dependency on software, hardware and cloud infrastructure.

The complexity of digitalization means that governments are fighting different battles — from "fake news" intended to influence elections to cyber-attacks on critical infrastructure. These include the recent wave of ransomware attacks on healthcare systems to the pervasive impact of a compromised provider of widely-adopted network management systems. Vital processes, such as the delivery of the vaccines in the months to come, may also be at risk.

Facing these heightened risks, decision-makers and leaders need to acknowledge that cybersecurity is a national security priority.

with high-value assets. In today's battles, governments have to adapt to fight against attackers that are silent, distributed, varied and technically savvy. The public and private sectors alike are engaged in this battle – and the private sector will need what only the public sphere can bring to the fight, including policy-making, market-shaping incentive models and training on a large scale.


How business leaders rate risks. Image: World Economic Forum's COVID-19 Risks Outlook

**2. Fragmented and complex regulations**

Cyber adversaries do not stop at countries' borders, nor do they comply with different jurisdictions. Organizations, meanwhile, must navigate both a growing number and increasingly complex system of regulations and rules, such as the General Data Protection Regulation, the California Consumer Privacy Act, the Cybersecurity Law of the People's Republic of China and many others worldwide.

Privacy and data protection regulations are necessary, but can also create fragmented, and sometimes conflicting, priorities and costs for companies that can weaken defence mechanisms. Within organisations' budgetary boundaries,

Individual regulations may have similar intent, but multiple policies add complexity for businesses that need to comply with all regulations, and this complexity introduces its challenges to cybersecurity and data protection, not always improving them. Policies must be creative in increasing protection while decreasing regulatory complexity. Cooperation among different policymakers is critical.

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:

- **Cybersecurity training:** In collaboration with Salesforce, Fortinet and the Global Cyber Alliance, we are providing free training to the next generation of cybersecurity experts. To date, we have trained more than 122,000 people worldwide.
- **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.

**3. Dependence on other parties**

Organizations operate in an ecosystem that is likely more extensive and less certain than many may recognize. Connected devices are expected to reach 27 billion by 2021 globally, driven by trends such as the rise of 5G, the internet of things and smart systems. In addition, the boom in remote work that began with the pandemic is expected to continue for many. The concentration of a few technology providers globally provides many entry points for cyber criminals throughout the digital supply chain.

The ecosystem is only as strong as its weakest link. The recent attacks against FireEye and SolarWinds highlight the sensitivity of supply chain issues and dependence on providers of IT functionality and services. Organizations must consider what the breadth of this exposure really means and must take steps to assess the real extent of their entire attack surface and resilience to threats. An inclusive and cross-collaborative process involving teams across different business units is vital to make sure there is an acceptable level of visibility and understanding of digital assets.

exacerbated this threat. Preventative measures for ransomware or any other cyber-attack should include preparation: presume you will get hit, back up IT resources and data, make sure there is continuity of operations in disruptions to computer systems, and drill and train the organization in realistic cyber response plans.

Businesses that actively adopt cybersecurity and more importantly improve their cybersecurity infrastructure are more likely to be successful. These businesses have come to see cybersecurity as an enabler to everyday operations. The significance of cybersecurity will likely only increase in the future in order to take advantage of the speed, scale, flexibility, and resilience that digitalization promises. Security by design and by default are becoming integral to success.

Organizational priorities should include a proactive plan for each business to build and maintain its own cybersecurity workforce. With security expertise becoming so difficult to source and retain, organizations should consider cultivating this talent organically. Organizations must also recognize that mobility is implicit in the modern technology workforce. It will be important to plan for the expected tenure of experienced professionals and recognize the long-term benefits that will accrue from a reputation for cultivating this expertise, transmitted from veterans to newcomers entering the field.

**5. Difficulty tracking cyber criminals**

Being a cyber criminal offers big rewards and few risks since, until recently, the likelihood of detection and prosecution of a cybercriminal was estimated to be as low as 0.05% in the US. This percentage is even lower in many other countries. Even when not obscuring criminal activity through techniques such as dark web tactics, it can be very challenging to prove that a specific actor committed certain acts. Cyber crime is a growing business model, as the increasing sophistication of tools on the darknet makes malicious services more affordable and easily accessible for anyone that is willing to hire a cyber criminal.

We have learned a lot over the last 18 months, and 2021 will be no different. We need to continue to adapt and take cyber risks seriously by planning, preparing and educating. Since it is a universal issue, open communications between corporations, policymakers, and regulators are a critical key to success. Until security features become integral to technology – seamless, transparent, and naturally usable by people – we will need to rely on business leadership to pay serious attention to cybersecurity.

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**

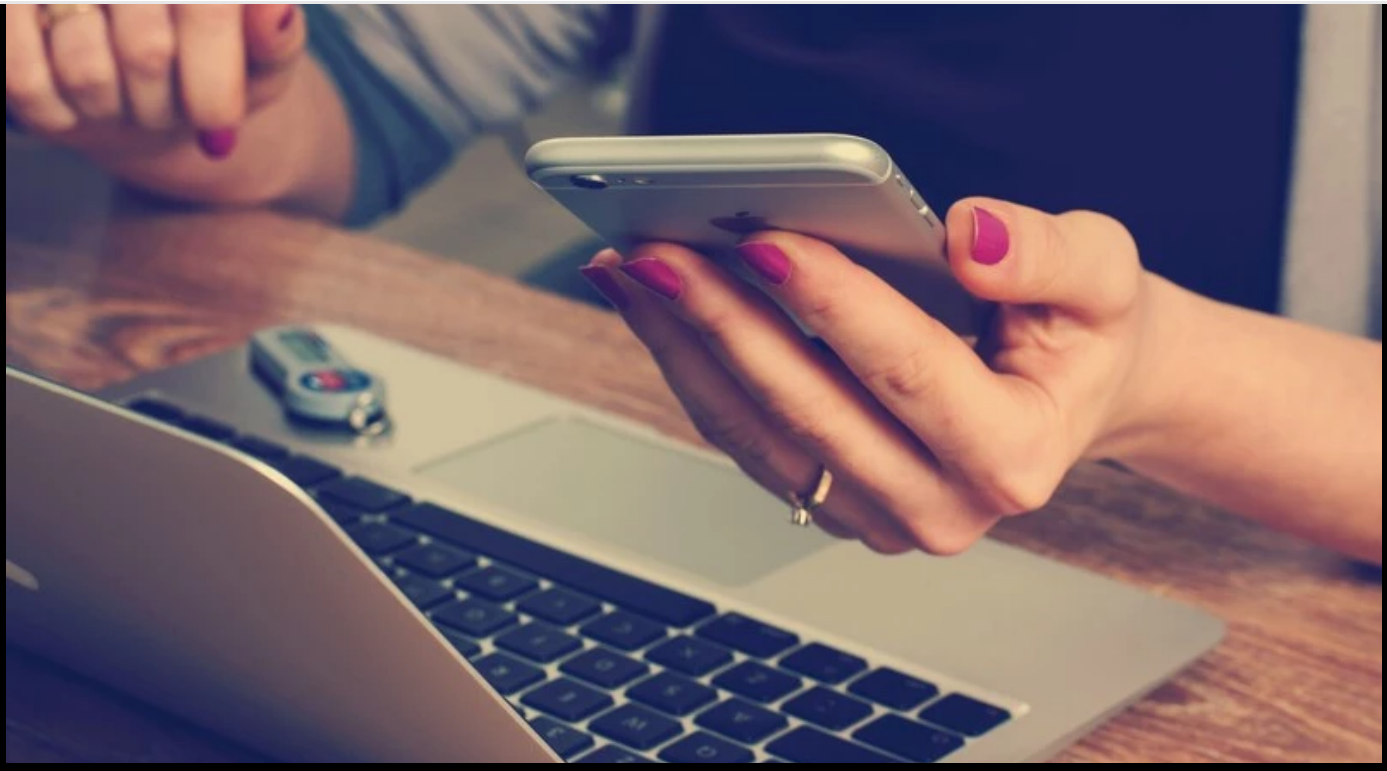
uplink

GLOBAL AGENDA

## **The Agenda** Weekly

A weekly update of the most important issues driving the global agenda

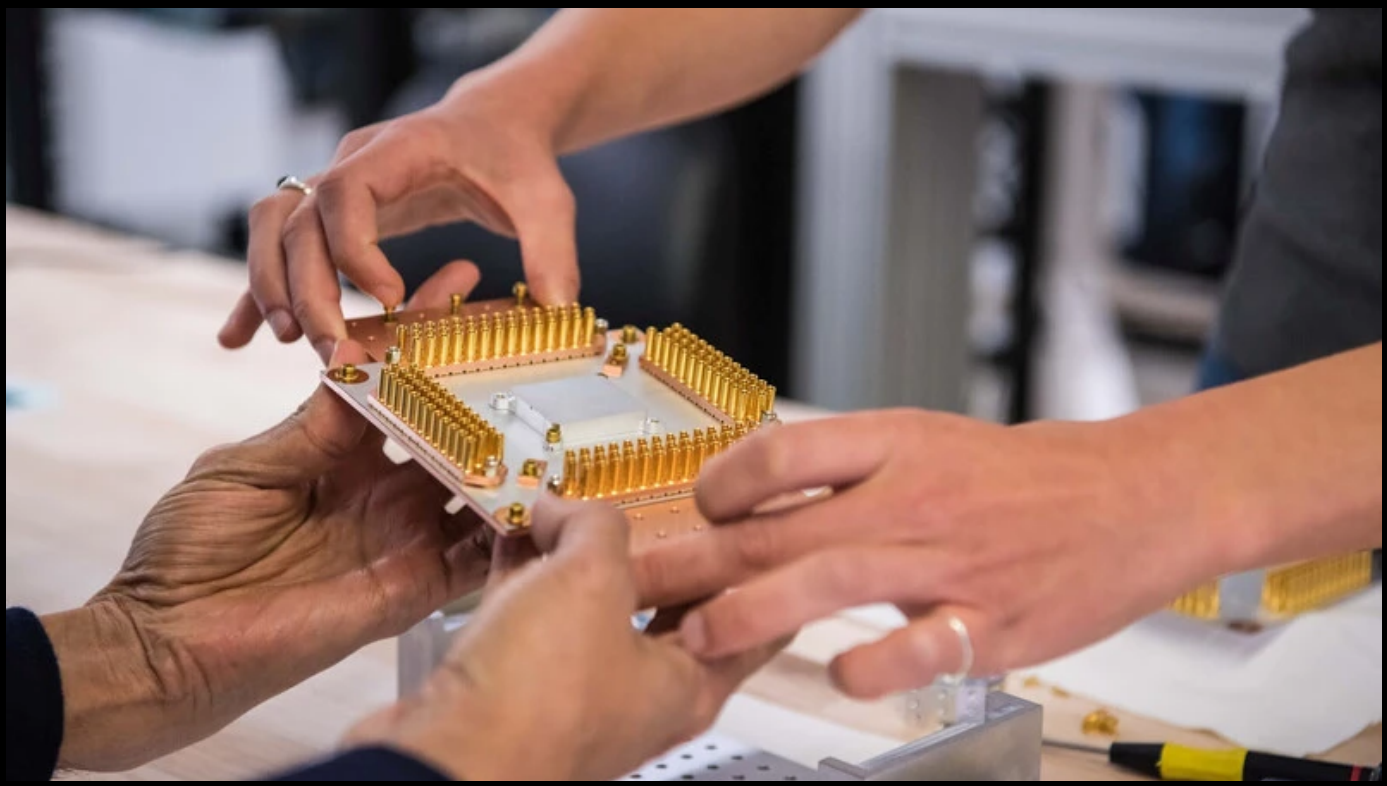
Subscribe today



## 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

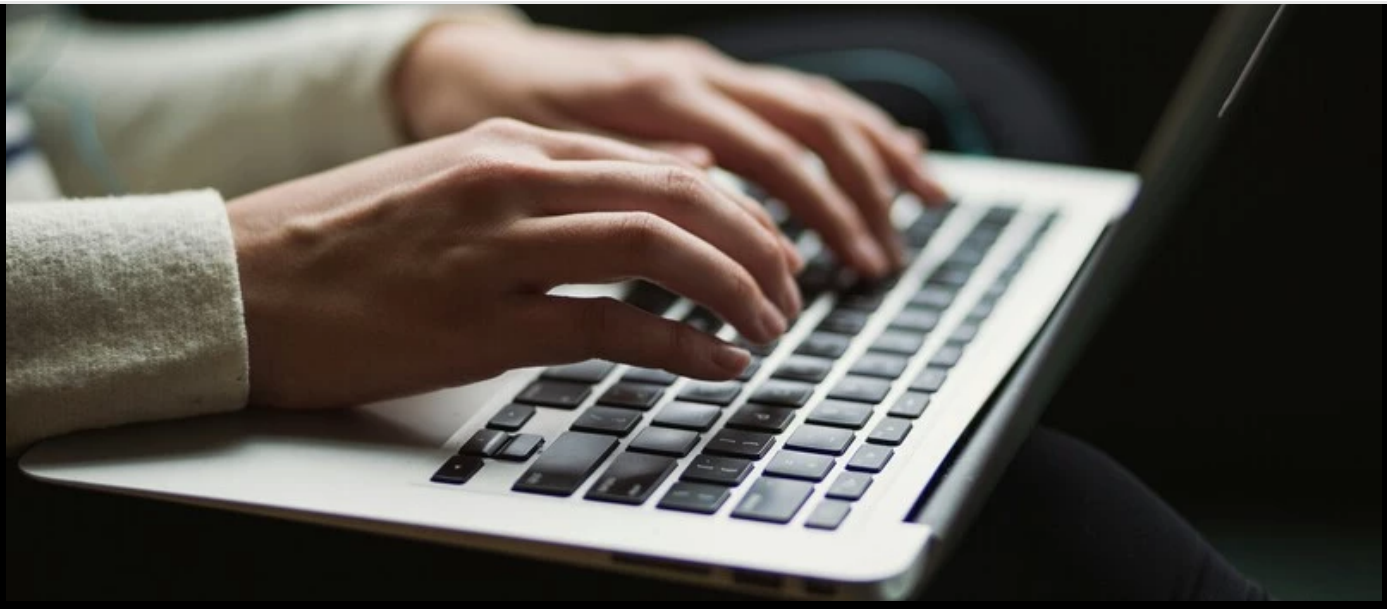
**Kesang Tashi Ukyab and Filipe Beato**

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

PARTNERS & MEMBERS

Sign in

Join Us

LANGUAGE EDITIONS

English

Español

中文

日本語