# Cybersecurity Trends

M. R. Pamidi, Ph. D. — Editor-in-Chief
Matt Pamidi — Creative Director
Praveen Pamidi — Director—Security
IT Newswire

Cybercrime reportedly cost damages totaling US$6 trillion globally in 2021, larger than the economies of U.S. and China and would be the world's third-largest economy, and is expected to grow by 15% CAGR reaching US$10.5 trillion by 2025.[1]

Cybersecurity is a journey and not a destination and security threats from hackers, fraudsters, phishers, and scammers are only expected to get worse and more frequent. Ransomware attacks, for instance, were three times higher in the first quarter of 2021 than they were during 2019, according to the UK National Cyber Security Centre. Sixty-one percent of respondents to a PwC research survey expect the ransomware attacks to increase in 2023. Ransomware locks files behind hard-to-break encryption and threatens to wipe them all if they are not paid.

With the explosive growth of containers and Kubernetes in the last decade, DevOps is at a crossroads when it comes to securing these diverse environments. Security and compliance requirements must be met before new apps can be deployed, but containers introduce new security challenges that existing DevOps tools and processes simply do not address. Thus, DevOps in many IT organizations, with emphasis on security, is morphing into DevSecOps—short development, security, and operations—which automates the integration of security at every phase of the software development lifecycle, from initial design through integration, testing, deployment, and software delivery. To emphasize, security must be built in from ground up. Thus, if IoT is a cake, security should be baked in like eggs, not schmeared on as an afterthought like icing.

Not only organizations but also individuals have become targets. Artificial Intelligence (AI) is coming to rescue cybersecurity professionals, as it did in financial fraud detection involving money-laundering schemes. AI can identify unusual patterns of behavior in systems dealing with hundreds of thousands of events per second. As IT security professionals encourage companies to invest in AI, cybercriminals are equally adept and aware of AI's benefits and will try to outsmart IT. In fact, they have developed new threats using Machine Language technology to bypass cybersecurity (think of 'sandbox'). Again, it'll be a battle of good vs. evil using the same technology—AI—and the savvy ones will win. This is not to discourage security spend, but to spend it wisely.

Phishing or spear fishing, either in the form of employees tempted to click on an innocent-looking link, thus welcoming malware, or via USB devices that employees pick up for free at trade shows, is also becoming more common. Stuxnet is one of the most well-known phishing incidents of the latter kind.

Finally, Internet of Things (IoT), about 27 billion by 2025 of which are expected to be connected by 2025 (Figure 1)[2], is another attractive pick for cybercriminals. The targets include billions of smart appliances, light bulbs, autonomous vehicles, and plant control systems (chemical, electric power, manufacturing, oil and gas, traffic, water supply…). Criminals have already hacked traffic signals in Washington, DC; government, energy, transportation, water, IT/communication, law enforcement/emergency services, financial, healthcare, media, and others—all targeted by Russia in Ukraine during the current war[3]; and the stock exchange in Estonia. Thus, IoT may have to be rechristened IoVT—Internet of Vulnerable Things.

[1] "Cybercrime damages set to total $10.5tn by 2025 warns SABIC official," ARAB NEWS, December 9, 2022
[2] "State of IoT 2022: Number of connected IoT devices growing 18% to 14.4 billion globally," IOT Analytics, May 18, 2022.
[3] "Winter is Coming: Russia Ups the Cyberattacks as Ukraine War Intensifies," Cyware Social, December 7, 2022.

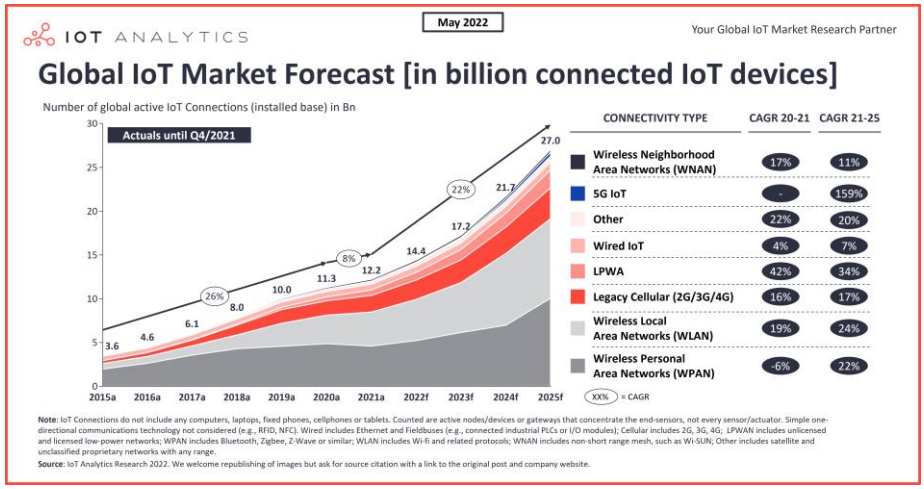


Figure 1. Global IoT Market Forecast (in billions of connected IoT Devices)

## Summary

The Cybersecurity industry is never dull and 2023 will be no different.

Cybersecurity will face more challenges with hacksters (hackers + fraudsters) trying to outsmart cybersecurity experts. Central governments have to play a key role to avoid individuals (seeking fun, money, or both) or state-sponsored infrastructure meltdowns. While our Defense Brass is stuck in 20th century warfare (mass killings, carpet bombing), the 21st century will face cyber warfare. Einstein is famously reported to have said, "I do not know with what weapons World War III will be fought, but World War IV will be fought with sticks and stones." We beg to disagree with probably the greatest scientist and humanitarian of all time and state: *The next World War will be fought with '0's and '1's. It will be a cyberwar. Mass Destruction of past wars will be replaced by Mass Disruption.*