CREATE A CLEAR 2020 CYBERSECURITY VISION

Four Cybersecurity Trends to Know

CYBER SKILLS GAP

The shortage of cybersecurity professionals is nearly three million globally with close to half a million in the U.S. alone. 60 percent of those professionals stated their companies are at moderate or extreme risk of cybersecurity attacks as a result of this shortage.[1]

THE POTENTIAL FOR MASSIVE ATTACKS ON IOT

With the mainstream adoption of the Internet of Things and the Industrial Internet of Things comes the potential for colossal security breaches. Businesses must continue to do their part to address new vulnerabilities and ensure these connected devices are secure.

AI-GENERATED CYBERSECURITY

Attackers are increasingly utilizing AI to mimic people we know, but security companies are also using AI to combat cyberattacks. In fact, 61 percent of enterprises say they cannot detect breach attempts today without the use of AI technologies and 48 percent say their budgets for AI in cybersecurity will increase by 29 percent in FY2020.[2]

GROWING DATA PRIVACY CONCERNS AND REGULATIONS

Data continues to be collected from every connected device which raises the question: who owns the data? If an enterprise possesses the data, then the enterprise must be mandated to protect it. The GDPR and CCPA will establish precedent for data privacy standards. New legislation will continue to be released.

SOURCES:

1 "CYBERSECURITY PROFESSIONALS FOCUS ON DEVELOPING NEW SKILLS AS WORKFORCE GAP WIDENS," (ISC)² CYBERSECURITY WORKFORCE STUDY, 2018.
2 "WHY AI IS THE FUTURE OF CYBERSECURITY," FORBES.COM, 07/14/2019.

E-mail securityservices@techdata.com to learn more about the current cybersecurity landscape.

TechData

Security Solutions