SUPPLY CHAIN connect™

BRIDGET MCCREA | Contributor

Increase in Cyberattacks Fueling Cybersecurity Market Growth

Data breaches hit an all-time high last year. Here's how companies are using technology to address this growing concern.

CDK Global is the latest of many organizations to be hit by cybercriminals this year. This time around, the ransomware attack brought an entire dealership management system (DMS) to its knees. According to *CBS*, fallout from the attack lasted for weeks for the 15,000 car dealerships that use CDK's sales, inventory management and customer relations systems to run their businesses.

Just as CDK was working to recover from the first attack last week, it was struck by a second attack. "Late in the evening of June 19, we experienced an additional cyber incident and proactively shut down most of our systems," CDK told *CRN.com*, which said that the system shutdown "resulted in an outage that has severely affected thousands of car dealerships."

While obviously monumental for the company that was attacked, the dealers that rely on its products and services (and their end customers), this was far from being an isolated incident. With digital transactions now commonplace for most industries, in fact, the number and intensity of cyberattacks appears to be growing exponentially.

Last Year's Solutions Won't Cut it

In a new cybersecurity risk report, MIT discusses how cybercriminals are finding new ways to exploit personal and business data. Data breaches increased by nearly 20% in the first nine months of 2023 compared with all of 2022, it says, during which time ransomware attacks escalated by almost 70%.

In fact, MIT says data breaches hit an all-time high in 2023—a trend fueled by increasing online interactions that put personal data in the crosshairs of criminal activity. As a result of these threats, cybersecurity has "escalated from an IT-level discussion to a C-suite and boardroom issue, with worldwide spending on security and risk management projected to hit $215 billion in 2024," MIT says.

Still, hackers are finding more creative ways to bypass security measures, motivated by the troves of unencrypted personal data being collected and stored in enterprise systems. "Most companies are aware of the threat and are doing things to improve security, but the bad guys haven't stayed still either," MIT's Stuart Madnick said in the report. "You have to think beyond what you did for protection last year."

OT Security Comes to the Forefront

Industrial operations are increasingly under threat as the industrial world embraces waves of digitization and smart manufacturing trends. Operational technology (OT) attacks are a growing concern, ABI Research reports, due to their more frequent, widespread nature.

By definition, OT cybersecurity safeguards operating technology assets, systems and processes from cyberattacks while also complying with strict regulatory requirements. In its report, ABI says the OT cybersecurity market is on track to grow from $12.75 billion in 2023 to around $21.6 billion by 2028.

It says network security and segmentation technologies will experience the most growth, followed by identity and access management and end-point protection.

"Every industrial sector imaginable is embracing some digitization and concept of Industry 4.0. As a result, the potential for cyber threats has also increased, prompting a growing demand for robust defensive measures," ABI's Michael Amiri said. "This market has lots of space for growth, as there is considerable capacity to expand smart industries."

For example, ABI says cybersecurity professionals are talking about how OT and Internet of Things (IoT) spending could surpass IT spending in the future, as the number of laptops, tablets, and other IT-related devices has hit a plateau.

"The fact is that OT and IoT devices are just beginning to expand and are far more numerous," Amiri explained. "An industrial plant could have tens of thousands of sensors, routers, and PLCs, all of which must be protected from malicious actors."