CONTRACTOR

TECHNOLOGY

Is the Construction Industry the Next Big Cybercrime Target?

68 percent of construction executives have no cybersecurity measures in place.

MAR 29, 2021

By Juta Gurinaviciute, CTO at NordVPN Teams.

The construction industry may not appear to be an obvious target for cybercrime, but it garners unwanted online attention just like other sectors. According to the Cost of Data Breach Report 2020 by IBM, the average cost of a data breach in the industrial sector was $4.99 million.

GlobalData, a data research company, predicts that the industrial sector's value will soar to $12.9 trillion by 2022. After rising consistently by 3.6 percent since 2018, it has now caught the eye of cybercriminals. Over half of all construction executives

believe their firms will be hit in the future, yet worryingly, 68 percent of firms have no security measures in place.

Growing attacks on industrial control systems (ICS)

The industry's vulnerabilities were exposed on both digital and operational levels recently, as cybercriminals attempted to compromise water treatment plant networks and poison the water supply in Florida. Most devices had a basic network connection, meaning heavy machinery could've been commandeered, leading to disastrous consequences.

IBM's X-Force Threat Intelligence Index 2021 has observed a 49 percent annual increase in industrial control system (ICS) attacks.

Other cybercriminals may aim for digital assets transferred or stored insecurely. Workers are increasingly dependent on digital tools in everyday operations. Innovative building firms employ Building Information Modeling (BIM) as a central database for blueprints, designs, and other assets. BIM is also used for collaboration with stakeholders from different building-related areas. Using devices and construction tools that are connected, workers can update BIM in real-time, improving communication and efficiency. Though, the amount of end-point devices mean the risk of exposing sensitive information is extremely high.

"The construction industry is heavily interconnected. Several building sites need to exchange data with headquarters and routinely access cloud services. Most workers use laptops and other end-point devices, with architects, engineers, and sub-contractors contributing online. The building industry isn't manual labor anymore — it's a sophisticated and digitally-managed trade, using high-end innovations and tools", says Juta Gurinaviciute, the Chief Technology Officer, NordVPN Teams.

Data breaches primarily affect company processes, resulting in prolonged downtime and operational disruption. Verizon recently found that only 5 percent of data breaches are caused internally, whereas external factors cause 95 percent. Security

teams should implement segmented network solutions such as virtual private networks (VPN) to strengthen their corporate IT infrastructure.

Protecting corporate networks and data

Secure the mobile workforce. Remote-working is relatively commonplace for builders shifting between different construction sites. If workers need assets from the cloud or a corporate network, make sure they're accessing them via an encrypted and secure VPN connection.

Establish a protected network. Building projects rely on teams constantly communicating with each other. All manner of different assets pass through networks that are often unprotected. A business VPN puts all workers and building sites within a secure software-defined perimeter and safely protected from outside threats.

It should also be established whenever construction ceases. Connecting smart sensors to a VPN will hide the network and protect it against cyberattacks.

Check third-party stakeholders. Building developments involve contractors, sub-contractors, architects, consultants, and clients — all parties communicating regularly.

"The more contributors to the project, the higher the risk of cyberattack. Only one compromised device is needed to hijack the systems of others. Before providing a third-party with access to your corporate network, make sure robust cybersecurity measures are in place. A standard VPN connection is a good option", says Gurinaviciute.

Ensure general cybersecurity. Some business VPNs provide custom gateways for different teams and branches. It enables access to cloud resources or company servers but directs traffic from other building sites separately. Contractors are also responsible for installing and setting up smart control systems on their network. It's their responsibility to maintain security, regularly update default passwords, and lead by example for the rest of the industry.

Juta is an IT professional with over 20 years of experience in cybersecurity and systems engineering. Currently, she is a Chief Technology Officer at NordVPN Teams. Prior to NordVPN Teams she held senior UNIX System Administration positions at Telia Company and Barclays. Juta is also a certified RedHat Systems Engineer.
