CYBERSECURITY POLICY AND INCIDENTS BRIEFING

ICYMI: Intelligent Buildings spotlights a recent event that highlights the need for **vendor compliance and oversight**.

SUMMARY

In the first week of August 2021, DataBreaches.net was contacted by a threat actor who claimed they had penetrated and attempted to extort ENE Systems, an HVAC vendor. According to the threat actor, they still had access to ENE Systems' networks and clients after ENE Systems became aware of the breach. One of these clients was Boston Children's Hospital. ENE Systems allegedly claimed that, though they were aware of the breach, they were unconcerned about the risks it posed to their networks and clients.

ENE Systems did not immediately respond to Information Security Media Group's request for comment about the incident. However, evidence was provided from the threat actor, including screenshots of schematics and wiring systems that were taken from Boston Children's Hospital. This evidence was captured from within ENE Systems' network.

WHAT IT MEANS

The response from EME Systems is not uncommon, as the lack of concern from most building control system contractors is typical and puts **all** contractor-managed systems at risk. Most organizations do not know how a contractor will (or won't) respond to a breach until after an incident occurs.

You can prepare by performing contractor audits that focus on:

- Remote access
- System and network backups
- Password and user management
- Security programs
- Incident response
- Review service agreements

HOW INTELLIGENT BUILDINGS CAN HELP

We have assessed the cybersecurity and vendor risk across thousands of buildings globally. In our experience, most building owners don't know what building control systems are connected, how they're configured, and what their recovery strategies are. Intelligent Buildings can **assess your buildings and provide ongoing Managed Services** to ensure your systems stay protected. Our Remote Access Management provides secure connection for all operators. Backup Management ensures centralized and up-to-date backups to restore building systems in case of emergency. Policy Compliance Management ensures best practices are being followed and **brings your systems and contractors into compliance**.