Replace Phone Lines with IP or Cellular Alarm Communications

Upgrading intrusion and fire control panels to use IP or cellular communications lowers costs, and enables higher security, faster data transmissions and new recurring monthly revenue opportunities.

Alarm communication technology is changing. Telecom companies are attempting to replace damaged copper lines with newer technology, and wireless and Internet-based phone services are taking the place of traditional phone lines. These changes can disrupt service at sites with intrusion and fire alarm control panels that are using older technology for alarm communications.

While some view communication technology changes as a significant challenge, others see them as an opportunity. A tremendous amount of intrusion and fire alarm control panels installed throughout the U.S. are currently communicating over PSTN. With a simple upgrade, these panels can take advantage of more modern technology to send reports to the monitoring center's receiver via Ethernet and/or cellular connections.

Dialer capture devices, like the UL 864 listed B465 Universal Dual Path Communicator from Bosch, can convert a control panel's PSTN digital dialer to an IP signal for transmission over Ethernet or cellular network.

Benefits to Upgrading
Upgrading panels to communicate over IP or cellular technology reduces communication failures caused by the aging PSTN infrastructure, lowers costs for users, and enables higher security and faster data transmissions. Let's take a closer look at each of the benefits for alarm communications using IP or cellular.

Reduced Costs
Eliminating the expenses associated with up to two dedicated telephone line connections per control panel results in a lower total cost of ownership for fire or intrusion alarm systems for users. The monthly cost for a telephone line varies depending on the provider and the location of the user, but cellular data plans for control panel communications are consistently less expensive than POTS lines, providing a savings for the user. For a user with multiple sites – such as a chain with hundreds of stores or restaurants in a region – this can add up to significant savings and a rapid return on investment for the system upgrade.

The availability of dialer capture devices that work with nearly any manufacturer's control panel enables security professionals to easily upgrade a wide range of panels. Modern dialer capture devices are able to automatically detect a panel's communication format for compatibility with a variety of legacy communication methods, such as Contact ID, SIA, Pulse 3/1, Pulse 4/2, Modem II, Modem IIe and Modem IIIa.

Higher Security
While PSTN dialers are tested for proper operation, it can be several days between tests, creating an opportunity for sabotage. Systems with IP and cellular connections are supervised more frequently. If the connection is lost, the monitoring center knows almost immediately. Also, the data transmitted is authenticated and can be encrypted to prevent intercept attacks. Because PSTN-based communications are not authenticated or encrypted, they can be disabled by recording and replaying signals or by substituting the alarm panel.

Faster Data Transmissions
Using IP and cellular with intrusion and fire systems provides higher speed communications compared with telephone dial up and ensures the panel will not encounter a busy signal from the receiver. These communication methods result in more data getting through faster to the people monitoring the security and safety of a building.

Important Considerations
When choosing a dialer capture device, consider compatibility, supervision, connectivity and programming options, and the ability to keep pace with technology changes.

Compatibility
Ensure the dialer capture device supports multiple formats to work with a range of panels from varying manufacturers.

Supervision
For enhanced safety and security, look for end-to-end supervision of the communications between the control panel and the monitoring center's receiver. Some devices will provide two acknowledgements – the first by the dialer capture device and the second by the receiver. This can cause confusion for the user who may think an alarm signal was received by the monitoring center at the time of the first acknowledgement. If an error occurs, the device may continue to try to communicate with the receiver and eventually create a communication failure notification. However, in the meantime, the user may believe the message has already been received.

Other dialer capture devices will acknowledge a signal only after it is received by the monitoring center's receiver. This end-to-end supervision loop eliminates confusion and provides the user with reassurance that the alarm communication has actually been received by the monitoring center. It also ensures faster notification when a critical communication does not make it to the receiver.

Connectivity and Programming Options
The ability to connect to the dialer capture device via the cloud can simplify remote connectivity without requiring a static IP address or DNS. Having the option to either connect directly or to use cloud connectivity enables your security professional to choose the method that best meets your needs and requirements.

It is also important to have the flexibility to configure the device locally, such as through a USB connection, or remotely via programming software when centrally-managed programming is preferred.

Future-proof Design
Support for IPv6 will be essential when IPv4 addresses become exhausted. Also, cellular communication technology must be easily upgradeable, as it changes regularly. An interface for plug-in cellular modules protects the users' investment, as the module can be changed to support the latest technology.

For more information on dialer capture devices like the Bosch B465 Universal Dual Path Communicator, visit www.boschsecurity.us