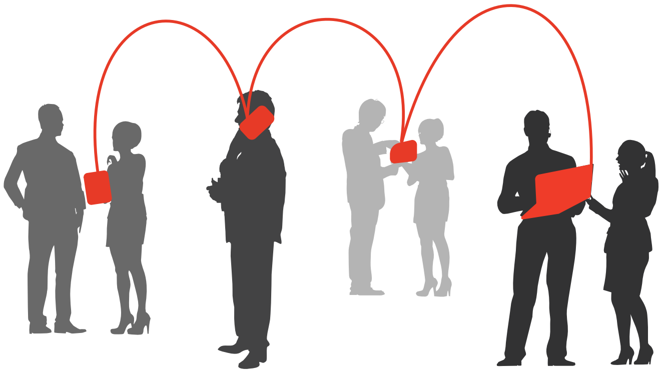
CISO'S GUIDE TO SECURING ENTERPRISE COMMUNICATIONS

ABIresearch for visionaries silent circle

Digital communication systems form an integral part of the critical infrastructure that underpin modern societies, and CISOs should be paying particular attention to the massive transformation coming on the horizon. These systems are expanding exponentially, connecting a broad range of devices, from smartphones to the Internet of things (IoT), across many sectors. By 2021, ABI Research forecasts 48.8 billion devices will be connected globally, including a broad variety of legacy and newly connected vectors, ranging from industrial SCADA networks to 4G connected wearables.

Beyond fiber and Wi-Fi, this expanded connectivity will take many forms, with wireless being the dominating sector by far: from short-range such as Zigbee, Z-Wave, and 6LoWPAN to longer-range cellular including LTE variants, and the upcoming 5G standard. These protocols will connect small, low-powered sensors with limited processing capabilities (such as actuators and controllers) to large complex machinery, like connected cars and supervisory control and data acquisition (SCADA) systems. All being linked back eventually to IP networks, back-end infrastructure, and IT systems for monitoring and management purposes.

The opportunities provided by this expanding ecosystem are exciting, but can only truly be realized if there is trust in the system. Trust plays a role in the manufacturing of devices and the provision of services. The information and communication technology (ICT) infrastructure is itself subject to sustained cyber attacks and constant exploitation by malicious actors. Connecting operational technologies to a digital landscape significantly increases risks, as new threat vectors could expose vulnerabilities in the functional safety of a device. A denial-of-service attack or ransomware, for example, could corrupt a critical function, such as the brakes in a car, or the dosage of insulin in a medical device, and the consequences may be deadly.



One of the difficulties for enterprises, in particular with the IoT, will be how to scale security in the most effective manner. Most importantly, security must become seamless, that is easy to use and to implement. With the expansion of connected devices, it can be a challenge to secure all potential vectors and minimize risk, especially given the diversity of systems in use. The trick will be for the market to provide a multi-platform, interoperable, and fully manageable technology that can unify security in the chaos that is created with the expanding ICT landscape. Above all, comprehensive enterprise protection can only be achieved through a combination of secure hardware, to anchor trust, and software, to enable flexibility.

Concretely, for CISOs, ensuring integrity and security of their communication network is a continuous effort. It means first determining the extent and usage of the communication channels in order to have the knowledge and visibility required to correctly assess the risk posed to their organization, based on their risk appetite. This requires a dedicated internal effort to map and analyze existing channels of communications, between people, systems, and devices. It also means anticipating new means of communications that may become standard channels on which core business is conducted. Such an exercise can be difficult, not least because some may belong to shadow IT. Therefore mapping communication channels also means finding out those tools that are being used without corporate approval.

Once this is done, it allows CISOs to put together a plan of action to plug the gaps and address vulnerabilities, for both approved and shadow IT. One of the primary elements to understand is that security cannot be guaranteed 100%. There will always be vulnerbailities and unknown risks, and CISOs must always take that knowledge into consideration. As such, a security strategy and accompanying implementation plan needs to address risk appetite and acceptance, what is allowed and what is not, how to inform and obtain approval for tools, incident response and remediation plans, and educational initiatives. Most importantly, such a strategy needs to be approved and endorsed at the top of the organization, and communicated throughout the enterprise so that all employees, and potentially outside contractors, understand the requirements.

Critically, organizations need to be doing this on a continual basis; mapping their communications channels on a regular basis and updating their strategy to reflect accurate usage. As organizations evolve and scale, priorities and risk appetite will inevitably change.

As such, CISOs will have to continually decide what they can do internally with their existing resources and what should be outsourced. The cybersecurity market generally is mature, but the growing enterprise IoT landscape keeps the industry on its feet. New solutions emerge regularly to address new vulnerabilities and threat vectors that did not exist previously. The market can provide some highly interesting solutions to enterprises large and small, in all types of sectors.

When considering vendors, CISOs need to also ensure those vendors address their pain points specifically, provide a solution that is fit for their purpose, and offer partnership-level support. Cyber threats are ever-evolving, requiring the need for cybersecurity to evolve as well. While a solution should minimize complexity in operation and management for the organization, the solution provider must also be a reliable and flexible partner, ever-present and work in tandem with the CISO’s security playbook. CISOs will be much better served by a supportive and comprehensive platform that adapts to their specific needs on a continuous basis.

Published January 31, 2018

©2018 ABI Research
249 South Street
Oyster Bay, New York 11771 USA
Tel: +1 516-624-2500
www.abiresearch.com

About ABI Research

ABI Research provides strategic guidance for visionaries needing market foresight on the most compelling transformative technologies, which reshape workforces, identify holes in a market, create new business models and drive new revenue streams. ABI's own research visionaries take stances early on those technologies, publishing groundbreaking studies often years ahead of other technology advisory firms. ABI analysts deliver their conclusions and recommendations in easily and quickly absorbed formats to ensure proper context. Our analysts strategically guide visionaries to take action now and inspire their business to realize a bigger picture. For more information about ABI Research's forecasting, consulting and teardown services, visionaries can contact us at +1.516.624.2500 in the Americas, +44.203.326.0140 in Europe, +65.6592.0290 in Asia-Pacific or visit www.abiresearch.com.

ABI Research is an independent producer of market analysis and insight and this ABI Research product is the result of objective research by ABI Research staff at the time of data collection. The opinions of ABI Research or its analysts on any subject are continually revised based on the most current data available. The information contained herein has been obtained from sources believed to be reliable. ABI Research disclaims all warranties, express or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.