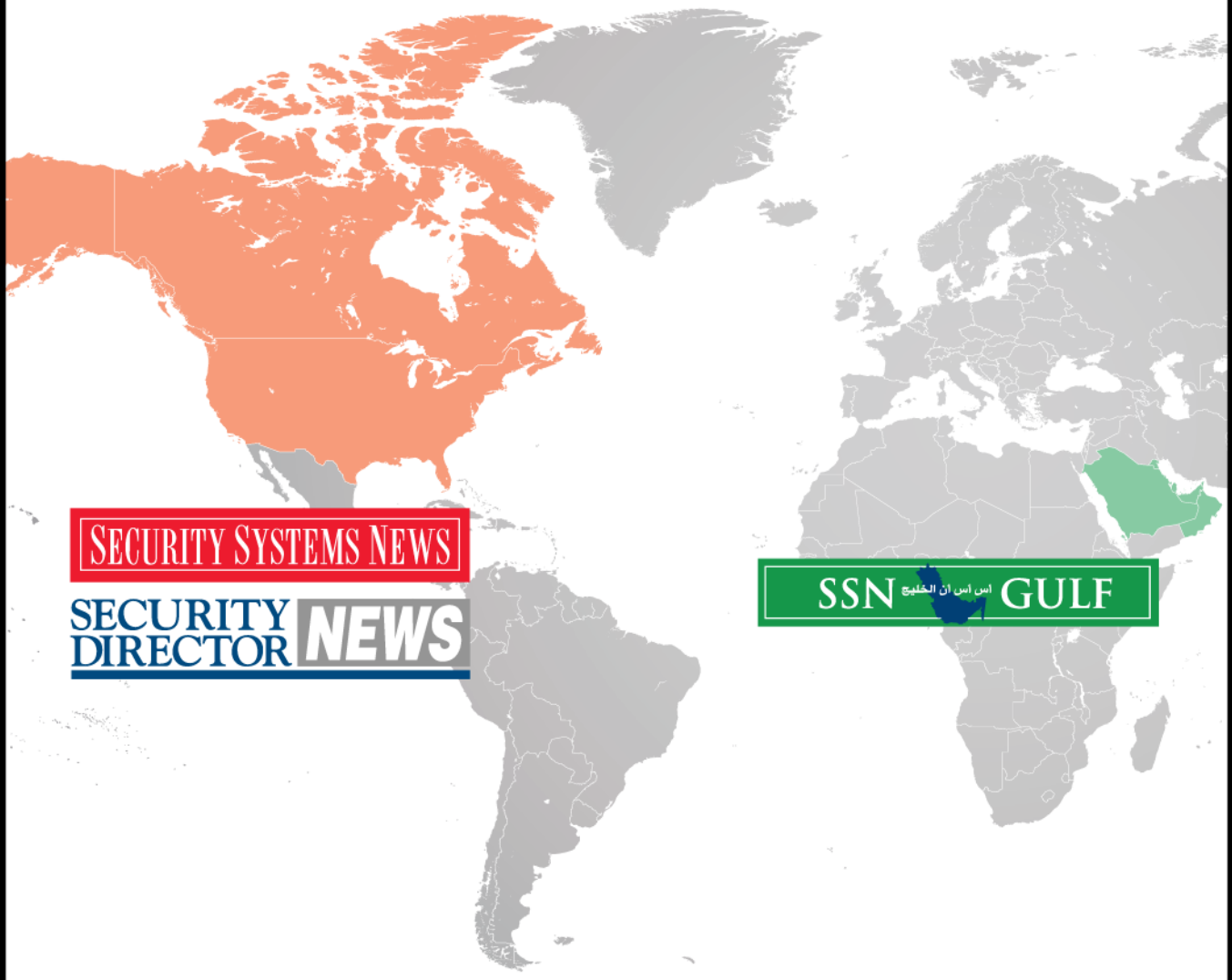
A SUPPLEMENT TO

SECURITY SYSTEMS NEWS

SIA FISCAL YEAR INFORMER

Q3 : 2014

Global Security News Coverage



www.SecuritySystemsNews.com

www.SecurityDirectorNews.com

www.SSNGulf.com

For more information, contact:

Tim Purpura
Group Publisher
tpurpura@securitysystemsnews.com

Cyber Threats to Physical Security Systems

By Jorge Lozano

We all know that critical infrastructure can be vulnerable to cyberattacks. Firewalls protect unauthorized access to and from a private computer network. These firewalls may need the support of other IT security appliances or devices to properly protect the complex networked information systems so that servers and computers are not infected by malware, viruses or other new threats, which have become increasingly sophisticated. These threats can penetrate and attack various edge devices, such as workstations and servers as well as mobile devices.

The reality is that most firewalls are not designed to protect electronic security systems (ESS) or supervisory control and data acquisition (SCADA) systems, from sophisticated cyberattacks, putting operating capability essentials at risk. We all are aware of the sophisticated attacks of the Stuxnet virus, which was designed to attack industrial programmable logical controllers (PLC); this ruined almost one-fifth of Iran's nuclear centrifuges. Each year, damage to critical infrastructure from network incidents and cyberattacks is measured by billions of dollars.

We also learned recently that some mobile cellular technology is very open to such attacks, and that includes a majority of edge devices that are connected to the networks, including home alarm and even medical devices.

Traditionally, ESS systems were not designed to be networked over IT infrastructure; ESS Systems have their own standalone networks. In the aftermath of 9/11, more and more ESS systems have been integrated into IT network infrastructures to get the most data from them, as well as to be more efficient in investigating crime and research of potential vulnerabilities.

Many hazards result from institutions' demand of more video-data and audio coming from the ESS systems, which results in growing numbers of physical security peripherals (PLC, RTU, controllers, microcontrollers, etc.) connected to the IT networks infrastructure of the facility. These networks are not fully capable to protect these systems, nor do some of the technical staff of these networks clearly understand these ESS systems in depth and detail. We are witnessing an increasing number of attacks on physical security systems that are connected to these networks. The need for a comprehensive solution is real.

Most ESS peripherals use a diversity of devices and subperipherals similar to SCADA systems, with proprietary embedded operating systems (OS). These peripherals allow the automation of electromechanical processes such as those used to control machinery on factory assembly lines and amusement rides, to open or close doors, and other ESS operations.

These peripherals are known in the security industry by specific names, depending of the manufacturer of the ESS, and most of them use the same technical foundation to operate. A minimum number of these peripherals meet standards like FIPS 140-2 from the National Institute of Standards and Technology, and most cannot protect properly against specialized cyberattacks. Their communication ports to their networks have vulnerabilities.

The use of these unsecured networks exposes ESS to cyberattacks:

- Video streams from cameras can be replaced or manipulated.
- Control can be hacked to open gates and doors.
- Perimeter security sensors and controllers can be disabled.
- Wi-Fi and other wireless communications can be disabled.

To address this challenge, which goes beyond the traditional use of firewall security, these ESS systems require a better tailored network protection solution for assorted zones of devices and peripherals. ESS systems have to be designed with a clear understanding of these new environments and the threats, with advanced IT security technical skills and understanding of the electronic security industry in mind, while being implemented without system downtime.

The use of cutting edge hardware, along with network intelligence and policy-enforcement software engines, offers an effective tool for securing and hardening sites and installations.

The ESS cybersolution acts as a powerful security policy enforcement tool, allowing the user to:

- Detect and identify every element and endpoint in network.
- Alert or block any attempt to connect an unauthorized device.
- Inspect all traffic at port level to make sure that only safe and identified traffic is allowed.
- Detect Layer 2 and Layer 3 cyberattacks: CAM overflow, ARP spoofing or poisoning, IP address spoofing, video hijacking, protocol manipulation, denial of service, etc.
- Report and take automatic action to restore continuous and safe operation of the network.
- Make the switch policy-enforcement tamperproof.

ESS systems and their infrastructure are at risk of cyberattacks. Existing network security protocols in place do not meet the needs to protect these systems.

Jorge Lozano is the CEO of Condortech Services, Inc. He can be reached at jlozano@condortech.com.