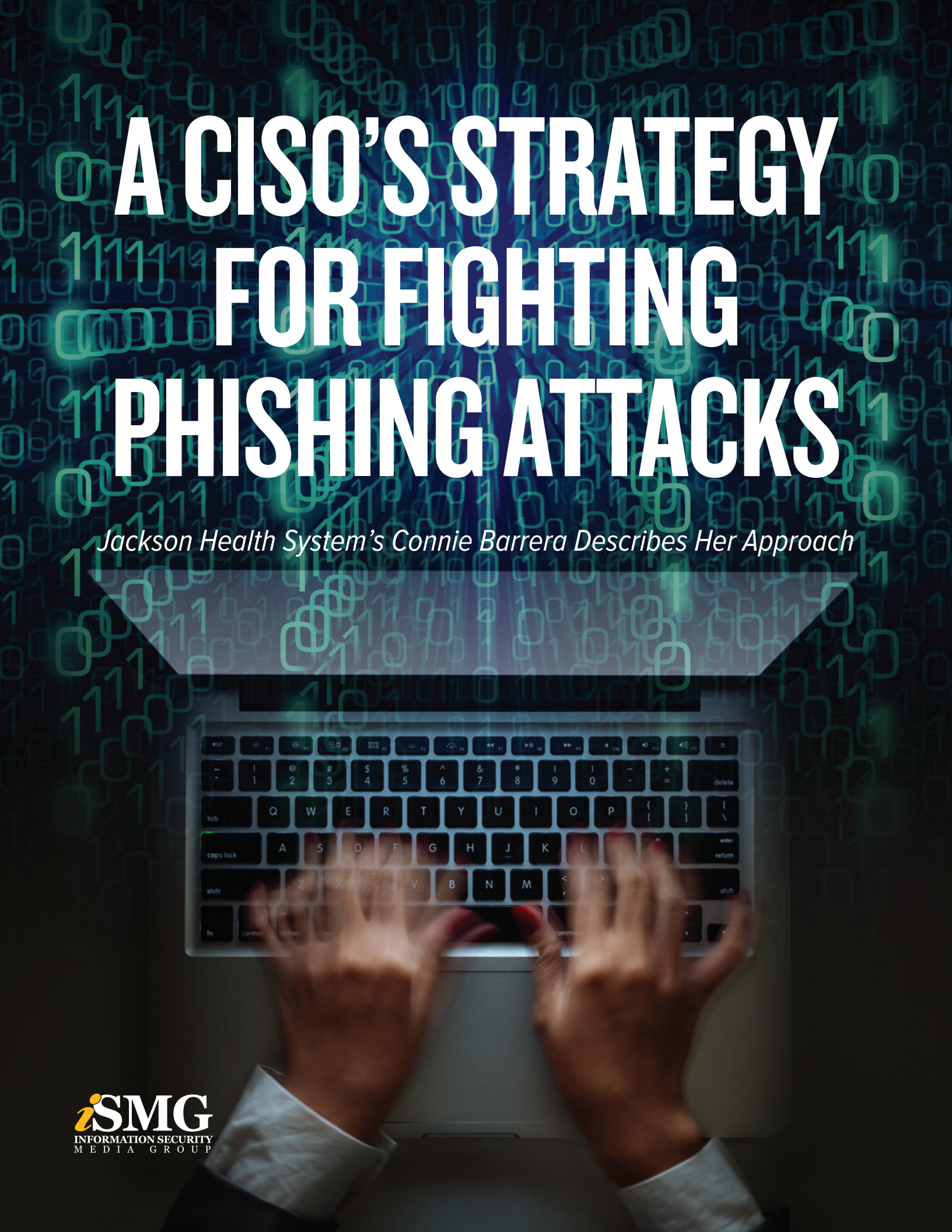
A CISO'S STRATEGY FOR FIGHTING PHISHING ATTACKS

Jackson Health System's Connie Barrera Describes Her Approach



ISMG
INFORMATION SECURITY
MEDIA GROUP

PhishMe® is the leading provider of threat management for organizations concerned about human susceptibility to advanced targeted attacks. PhishMe's intelligence-driven platform turns employees into an active line of defense by enabling them to identify, report, and mitigate spear phishing, malware, and drive-by threats. Our open approach ensures that PhishMe integrates easily into the security technology stack, demonstrating measurable results to help inform an organization's security decision making process.

More information is available at www.phishme.com

Hacker attacks often start with spear-phishing attempts used to obtain credentials or deliver malware. But healthcare entities can take steps to help prevent these scams from being successful, says Connie Barrera, CISO of Jackson Health System in Miami.

The delivery system, which includes several hospitals, clinics, mental health and long-term care facilities, combines technology and training in its anti-phishing efforts, Barrera says in an interview with Information Security Media Group.

On a periodic basis, Jackson Health sends fake phishing emails, using a product from PhishMe, to test whether employees will open them or click on the URL contained within the message, she says.

"Without anyone's knowledge we'll send a [test] email that [conceivably] could be malicious. A URL is embedded in the message and the software will track all actions," she explains. "For instance, the software will track if someone merely opened the email but did nothing else with it. It will also track whether someone clicked the link and went to the website, as well as if the person entered any credentials."

If a user clicks on the fake URL and enters credentials into the website, "it's our choosing of any educational material [to offer that user], she says." Sometimes it's an HTML page, sometimes it's an interesting video directly related to the content of the email. Other times it's a short game."

Immediate Feedback Essential

Barrera says testing whether users fall for the fake phishing scams is effective because the results and response are immediate. This approach, she argues, is far more effective than someone taking a class a long time after a phishing incident is discovered.
Staff members sitting in a training session listening to descriptions of phishing attempts typically say they'd never fall for those tricks, the CISO says. But things change when the users are actually faced with the real phishing email.
"It's a completely different world when they're sitting at their desk and it's only

Connie Barrera

"It's really critical to have a strategy for your communication. While no or poor communication is definitely a detriment to the organization, if the communication is overwhelming or too much, it just becomes noise."

them, their keyboard and their screen and they see a message [that says] 'we love our employees, we're giving you free coffee, let us know what kind of brew do you like?'" That's why combining the software phishing testing tool with security awareness training is an effective approach, she says.

Also, the training solution that Jackson Health uses includes material designed for the average employee, and also "micro-modules" for executives, "who are pressed for time on a day to day basis," she says.

Jackson Health couples that with one-on-one "walk-through" training sessions and other initiatives, such as email blasts and posters about security and privacy she says. "It's really critical to have a strategy for your communication. While no or poor communication is definitely a detriment to the organization, if the communication is overwhelming or too much, it just becomes noise."

In the interview, Barrera also discusses:

- Why the healthcare sector has become a hot target for hackers;
- Critical technology tools to help defend against cyber-attacks;
- Other steps Jackson Health is taking to guard against hacking attacks.

Barrera is director of information assurance and CISO at Jackson Health System. Previously, she held IT security and compliance leadership positions at the University of Miami and was lead IT auditor at Baptist Health South Florida.

Hear the interview

http://www.healthcareinfosecurity.com/interviews/cisos-strategy-for-fighting-phishing-attacks-i-2846

About ISMG

Headquartered in Princeton, New Jersey, Information Security Media Group, Corp. (ISMG) is a media company focusing on Information Technology Risk Management for vertical industries. The company provides news, training, education and other related content for risk management professionals in their respective industries.

This information is used by ISMG's subscribers in a variety of ways—researching for a specific information security compliance issue, learning from their peers in the industry, gaining insights into compliance related regulatory guidance and simply keeping up with the Information Technology Risk Management landscape.

Contact

(800) 944-0401

sales@ismgcorp.com

BANK INFO SECURITY® CU Just for Credit Unions INFO SECURITY® GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk TODAY CAREERS INFO SECURITY® Data Breach Prevention. Response. Notification. TODAY

ISMG INFORMATION SECURITY MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismgcorp.com