VOLUME 7, ISSUE 4
JULY / AUGUST 2017

change

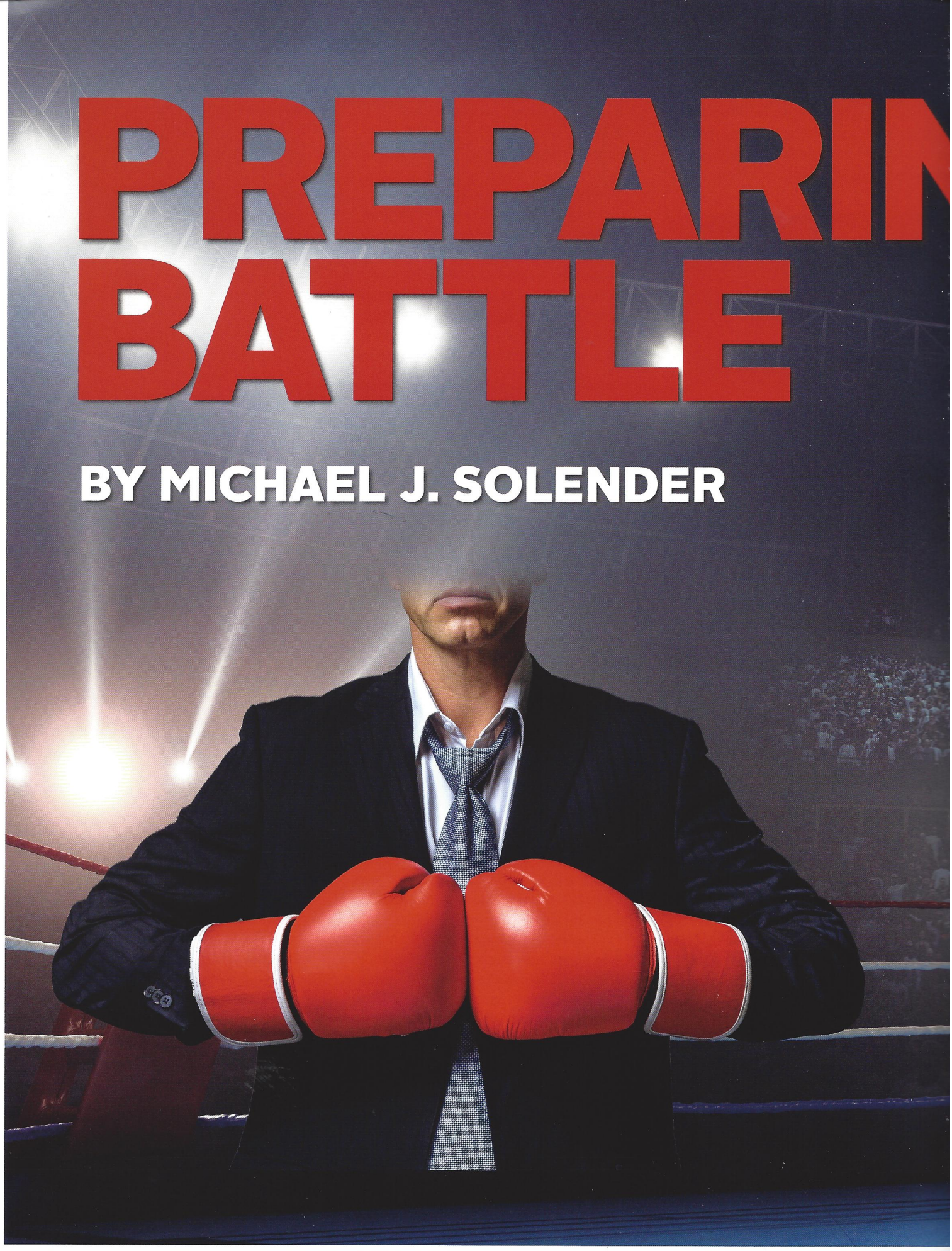
COMMUNICATION IN THIS AGE OF CHANGE

DIRTY WORK

THE ART OF BEING GRITTY

PREPARIN BATTLE

BY MICHAEL J. SOLENDER



G FOR

How organizations address gaps in their Information Systems security is critical to successfully fending off increasing cyber threats.

There are two types of companies: those that have been hacked, and those who don't know they have been hacked.

This oft repeated truism uttered by John Chambers, long-serving former CEO of IT systems at networking giant Cisco, has even greater relevance for organizations today than when the warning was first sounded nearly a decade ago. As organizations increasingly rely on information technology services and products to run their daily operations, the threats of malicious cyber hacking and system disruption pose a risk too great to ignore.

Cisco's 2017 Annual Cybersecurity report indicated that 29% of breached organizations it surveyed lost revenue. In addition to the financial losses, companies risk their reputation, intellectual property, client data and proprietary plans to exploitation from hackers.

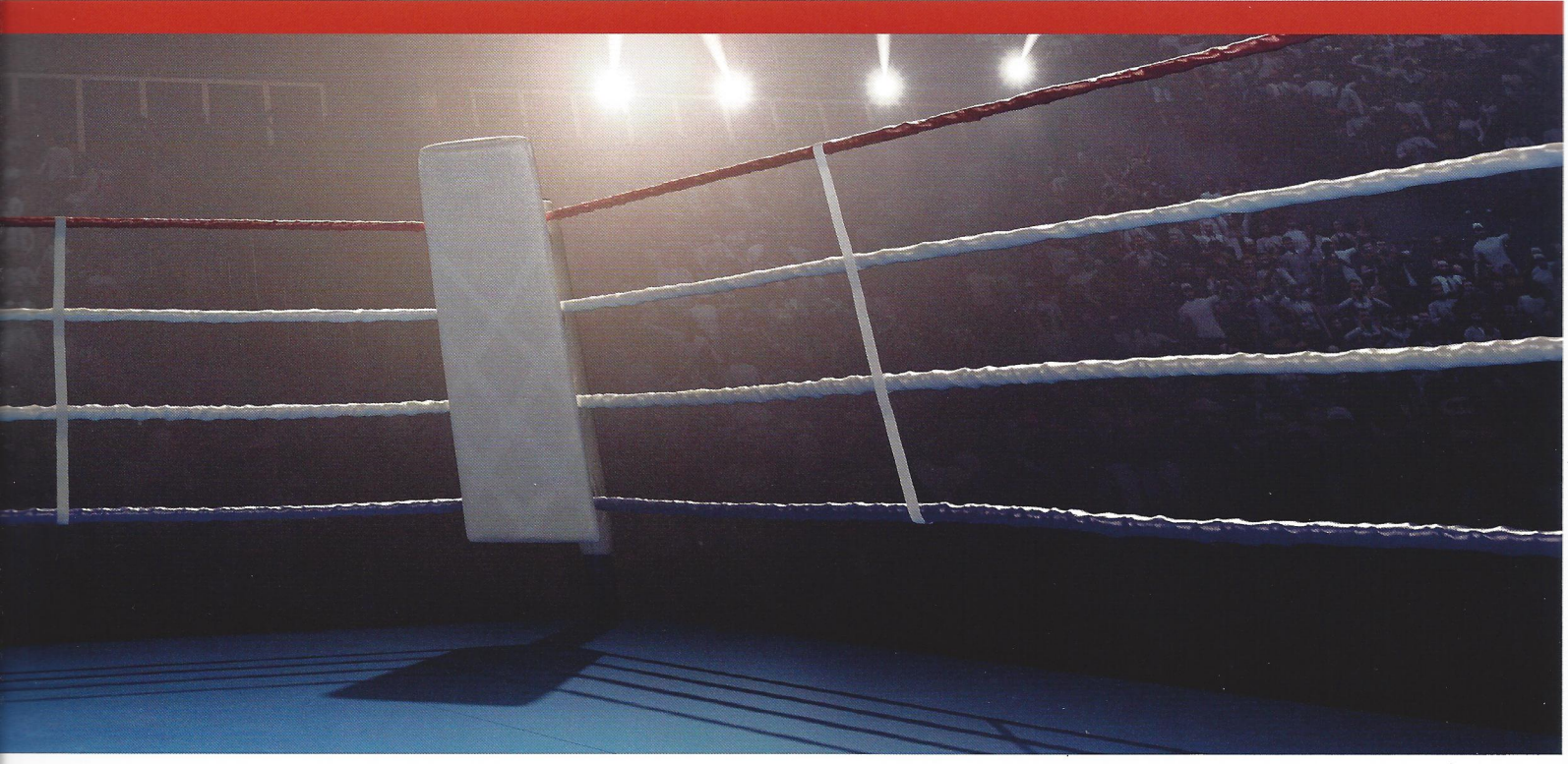
Most professionals point out that information security planning and prevention is far less expensive than remediation. Yet, many organizations continue to remain vulnerable in combatting this ongoing threat due to inadequate information security protocols, staffing and dedicated resources.

"Information security is a very real concern facing business today," said Spencer Coursen, founder and CEO of Coursen Security Group, a Washington D.C.-based threat management and security consulting firm. "Much in the sense that if Bonnie and Clyde were around today they wouldn't be bank robbers, they'd be hackers."

Minding the "information security" gap

Coursen noted, through his research and extensive experience conducting security audits of organizations, that he sees a tremendous gap regarding information security between organizations' plans and their actual capabilities.

"Putting smart policies into place isn't very effective if they aren't acted upon or the resources and tools needed to execute these policies aren't provided," Coursen said. He cited the 2013



data breach at Target stores as an example of an organization that had taken steps to head off security breaches but did not adequately execute their plans.

Target of course experienced one of the largest data breaches in the history of retail operations when an estimated 40 million credit and debit card numbers were hacked from their nearly 1800 storefronts nationwide.

As reported in the 2014 Bloomberg article "Missed Alarms and 40 Million Stolen Credit Card Numbers: How Target Blew It," Target had prepared for a malware attack prior to the data breach by installing a $1.6 million detection tool. Additionally, the retail giant retained the services of external data security monitoring services prior to the malware attack. With the appropriate safeguards in place, the company was notified when suspicious activity was detected, yet failed to act.

Several factors were identified in a post-mortem analysis, including the absence of a Chief Security Officer over Target's security operations center and the company's internal decision to switch "off" the option to automatically delete, without review, detected malware.

"There are many verticals in corporate security space these days – physical, data, cyber – but no real bridge that serves as a clearing house for these concerns," says Coursen. "With individual specialists calling their own plays, there's no consistency and uniformity across the organization. This makes staffing at the Chief Security Officer level critical. It's one of the biggest gaps I see, with no single level of accountability. Companies have to inspect what they expect, and having a functioning head with overall accountability for information security, regardless of the size of the organization, is a must."

Budgeting for information security

Budgeting for information security resources is an important way companies can address the widening gap between needs and capabilities.

"What we're seeing with most of the organizations we support is very limited resource allocation towards info-security and in many cases, none at all," said Heinan Landa, founder of Optimal Networks, Inc., a managed IT Services firm supporting small and medium-sized companies. "It's a question of resources. Most companies are doing the best they can to implement network operations best practices in terms of security, yet feel the expense burden. They see it almost like an additional tax. For those clients who have compliance requirements such as health-care organizations who are mandated by HIPPA to safeguard data, they take this seriously but not necessarily as their full-time job, often rather as an additional duty."

Landa says one of his foremost recommendations is that companies set up a dedicated budget line item for information security.

"We're saying it's critical to treat this separately and allocate dedicated resources," Landa said. "Companies are exposed whether they think they are or not. There is a level of risk that is exacerbated when organizations think they are not vulnerable or that their data does not matter to a hacker."

Finding information security talent

What's the right balance between internal and external IT security resources and how should companies best staff for their needs?

These are questions that require careful evaluation and assessment of an organization's current and future system needs and requirements. Small- and medium-sized organizations may find dedicated internal oversight of external resources is the best approach, while larger organizations may have a greater need for robust, dedicated internal security teams.

Regardless of need, a painful shortage of skilled IT security talent is a reality facing all organizations today. The nonprofit information security advocacy group, ISACA (previously known as the Information Systems Audit and Control Association) predicts a global shortage of more than 2 million cybersecurity professionals by 2019. Estimates of nearly 200,000 open cybersecurity positions in the U.S. on any given day are enough to give any organization pause. There are, however, steps companies can and should take, including committing to establishing an information security plan; assessing and evaluating software, hardware and human resources needs; identifying internal personnel responsible for overseeing security; and building in redundancy and training to their operations.

With cybersecurity positions growing four times faster than any other IT role, hiring and retaining talent continues to be a challenge.

Information Security Resources

- One good starting point for organizations looking for IT Security best practice standards is the **NIST special report: An Introduction to Information Security (https://www.nist.gov/publications/introduction-information-security)**. This report issued by the U.S. government's National Institute of Standards and Technology introduces the information security principles organizations can use to understand the information security needs of their respective systems.

- Cybersecurity certification such as **CISSP** (Certified Information Systems Security Professional) is a valuable education tool providing a depth and breadth of knowledge in many info-security areas including: Security and risk management, Asset security, Security engineering, Communication and network security, Identity and access management, Security assessment and risk, Security operations and Software development security. Find more information here: www.isc2.org/cissp..

CIO Magazine offered these tips to employ when selecting information security professionals:

- Keep an active social media presence – In other words, fish where the fish are. CIO advocates maintaining presence on social professional networks that are focused on verticals, like cybersecurity, and participating in the discussions there.
- Encourage and engage young talent – Mentoring and bringing along existing IT personnel, entry level analysts and those who show interest will deliver rewards for organizations willing to invest in growing their own.
- Offer more than salary – Look beyond compensation to recognize, reward and retain talented information security personnel. Underwriting continuing education and cyber security certifications, providing a learning environment at work and challenging personnel with leadership roles and project management responsibilities will all pay dividends.
- Avoid the "hard sell" – It's important to engage with information security pros on their own terms. Look to your internal IT staff or professional recruiters for outreach, engagement and opportunities to better understand the interests and desires of this community.

A readiness to combat information security threats is simply a necessary cost of doing business today. Tech-savvy companies recognize this and are investing in front end resources to best mitigate their costs.