› SECURING THE 'LIFEBLOOD OF TECHNOLOGY'

InfoSecurity PROFESSIONAL

SEPTEMBER/OCTOBER 2014

A Publication for the (ISC)² Membership

COMMUNITY!

A QUARTER CENTURY OF BUILDING INFORMATION SECURITY CAREERS AND CAMARADERIE

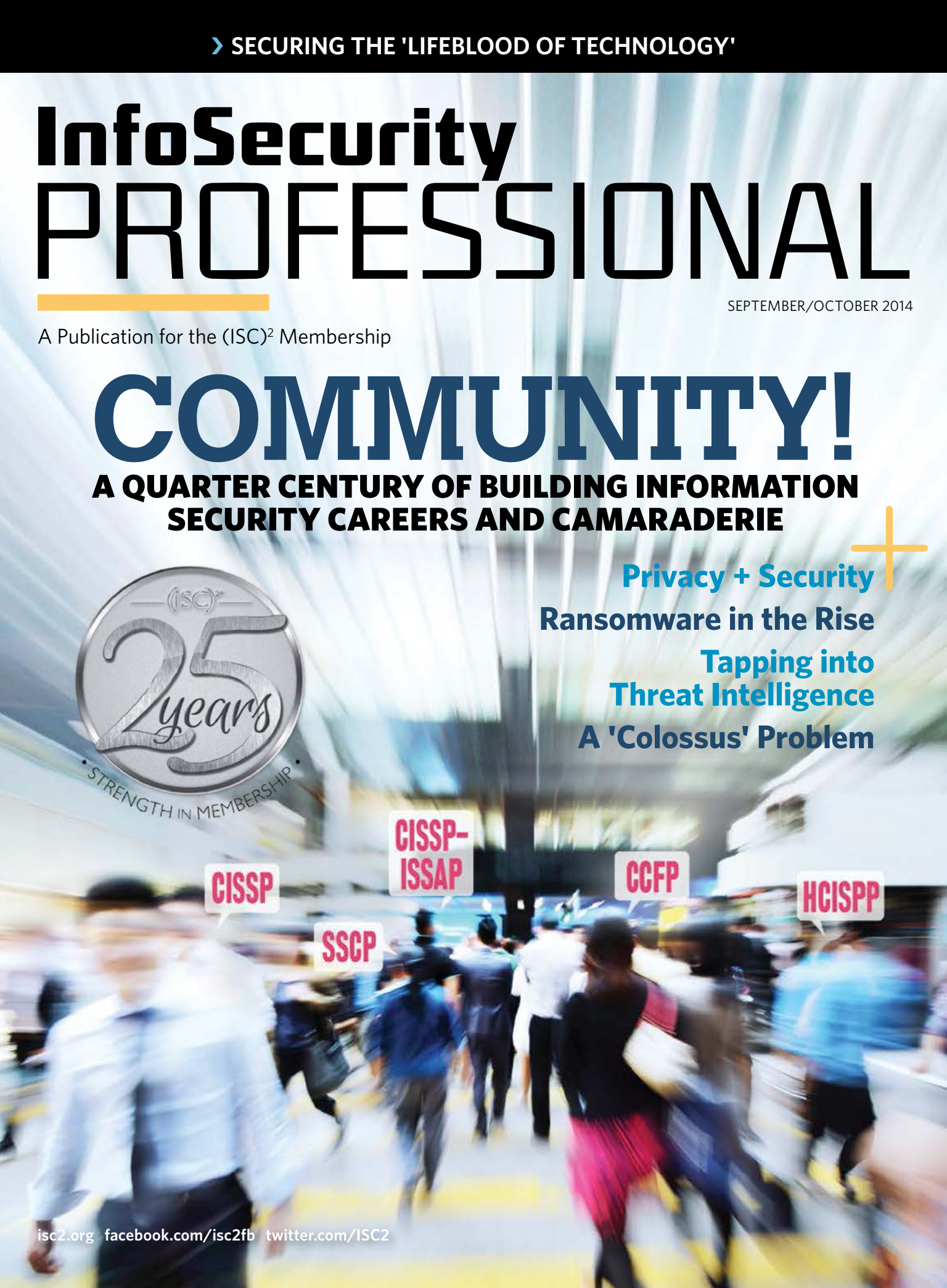
+

Privacy + Security

Ransomware in the Rise

Tapping into Threat Intelligence

A 'Colossus' Problem



GETTING LEFT OF THE HACK

HONING YOUR CYBER INTELLIGENCE CAN THWART INTRUDERS

BY **RANDY BORUM**

WHEN IT COMES to information security, it is easy to become so focused on what's happening inside your network that you neglect the outside actors that may be preying on your weaknesses. The knowledge of our adversaries' intentions, capabilities and activities in the cyber domain, or cyber intelligence, enables us to intervene before an attack occurs—or to get "left of the hack." Intelligence collection and analysis provide essential tools for staying ahead of the adversary.

Although the term "intelligence" may be unfamiliar or unclear to many traditional cybersecurity practitioners, both NIST's National Cybersecurity Framework (http://www.nist.gov/itl/csd/launch-cybersecurity-framework-021214.cfm) and DHS's Task Force on CyberSkills (http://www.dhs.gov/homeland-security-advisory-council-0) emphasize the value of the intelligence function.

Intelligence is not just a national security activity. It concerns a range of organizations in the private and public sectors. At the broadest level, intelligence might be thought of as "actionable knowledge," but as John Felker, director of Cyber Intelligence Strategy for Hewlett-Packard (Palo Alto, Calif., U.S.A.), points out, "intelligence for cybersecurity is more than 1s and 0s." Felker also co-chairs a national task force on cyber intelligence for the Intelligence and National Security Alliance (INSA) (http://www.insaonline.org).

Intelligence is not just a national security activity. It concerns a range of organizations in the private and public sectors.

The Cyber Intelligence Task Force uses a common three-part framework to describe the different levels at which actionable knowledge influences decisions and activities within an enterprise. The three overlapping levels are strategic, operational, and tactical *(see "Cyber Intelligence Task Force's Three-Part Framework," p. XX)*. The defining features of each level are based on the intended consumer, decision requirements, timeframe, adversary characterization, collection scope and methods.

The *strategic level* focuses on setting an organization's mission, direction, and objectives and developing a plan for how the organization will achieve those objectives. Intelligence collection broadly assesses the threat landscape for macro trends (e.g., political, social, economic) affecting the industry and the organization and discerns who the bad guys are, what they want to achieve, why, and how they will likely attempt to achieve those aims.

The *operational level* focuses on enabling and sustaining day-to-day operations and output, including logistics. At this level, cyber intelligence looks at the organization's internal operations and collateral partners and at external threats posing the greatest risk to business continuity and with the greatest potential business impact. Those analyses inform risk-based decisions about resource allocation and defensive actions.

The *tactical level* focuses on the specific steps and actions the organization takes to protect assets, maintain continuity, and restore operations. In the cyber domain, the tactical level is where on-the-network actions take place and where malicious actors and network defenders maneuver actively against each other. Intelligence examines the technical/logical tactics, techniques and procedures (TTP) used to target the organization.

The three-level framework—strategic, operational, and tactical—illuminates the "big picture" of cyber intelligence. Too often, "threat intelligence" focuses only on the tactical level: the technical dimensions of an attack such as implants, tools, and artifacts. There is no question that this information is valuable, but it is only one dimension of actionable information in cyber defense. Cyber intelligence must collect and analyze more than network logs; it must go beyond the network.

Developing Smart Defenses

Cyber intelligence should drive the cybersecurity mission and form the foundation of effective cyber defense. An intelligence-led approach can transform the organization from a reactive to a proactive security/risk management posture.

With finely honed cyber intelligence, an organization can align valued assets with prioritized threats and available resources. Troy Mattern, deputy head of cyber security for Zurich Insurance Group, describes the traditional cyber defense posture as a "Maginot Line," a static approach in which the central guiding principle is to "defend everywhere."

Mattern says that "risk-based, intelligence-driven security allows you to focus not just on generic threats and risks but your threats and risks. You have to know the specific risks that threaten your organization and develop your strategy around them. You can't do that without intelligence."

CYBER INTELLIGENCE TASK FORCE'S THREE-PART FRAMEWORK

Strategic Cyber Intelligence is:

- ✓ Produced for senior leaders at the C-Suite level in both private and public sectors;
- ✓ Used to maintain a competitive advantage and to inform the development of organizational/national strategy and policy that will direct the organization, often over the long term (3+ years);
- ✓ Collected broadly within the sector to which the organization belongs and likely includes complementary sectors (e.g., R&D and manufacturing, supply chain);
- ✓ Focused broadly on threat vectors and adversaries that include nation and non-nation state actors with intent and capability and on contextual political, economic, social trends; and
- ✓ Generally non-technical in nature, focusing instead on inter/intra sector trend analysis, stated and unstated objectives of nation and non-state actors, and other strategic indicators.

Operational Cyber Intelligence is:

- ✓ Produced for executive managers in IT and security, such as the CIO and CISO;
- ✓ Used to inform risk-based decisions about resource allocation and activity to maintain business continuity and prevent disruption, often for the foreseeable near-term;
- ✓ Collected with an emphasis on the specific organization/enterprise and operations to include partners, suppliers, competitors, customers and other trust relationships;
- ✓ Focused on targeted, opportunistic, and persistent vectors that pose the greatest risk to business continuity and that would have the greatest business impact; and
- ✓ Blends technical and non-technical collection to explore and prioritize organization-specific threats, the mechanisms and signatures of potential attacks, and the vulnerability of the organization's layered defense.

Tactical Cyber Intelligence is:

- ✓ Produced for incident response teams;
- ✓ Used to restore operations quickly and collect relevant evidence about the attack in an immediate timeframe;
- ✓ Collected with more of an internal emphasis on the organization/enterprise personnel, assets, and networks ("inside the wire");
- ✓ Focused on understanding and analyzing the adversary's use of technical/logical tactics, techniques and procedures (TTP) to target the organization; and
- ✓ Generally more technical in nature focusing on the implants, tools, delivery mechanisms, and technical/logical artifacts of an attack.

A Roadmap to Cyber Intelligence

At the core of a risk-based, intelligence-driven security approach is a function that continuously collects, processes, analyzes, and disseminates information about the vulnerability of valued assets in relation to the risk posed by internal and external threats and uses that information to guide its decisions and operations. There are several steps organizations can take to achieve an intelligence-led approach to cyber defense.

- **Approach Cyber Defense as a Dynamic, Ongoing Process:** After WWI, France built the Maginot Line, a massive fortified wall, along its border with Germany. The rationale for building the Maginot Line was very similar to the rationale for deploying firewalls today—to provide time for their army to mobilize in the event of attack. But in response to the Line, the Germans just changed their attack strategy. They adopted an approach based on speed and surprise rather than direct, frontal assault. The Germans went around the fortress and attacked France from Belgium. The Line did not falter, but by itself, it could not defend against the intrusion.

Just as the Maginot Line could not defend against ever-changing intrusions, neither can firewalls. Information security methods have evolved considerably since the early days of broad, static perimeter defense. Security assessment and response must be a continuous process, and security mechanisms must be multi-layered and dynamically deployed. Adversaries adapt, and they will prevail without a dynamic defense.

- **Look Beyond the Network:** Most security teams say that they monitor "threat intelligence," but those activities occur almost exclusively on the network. Organizations must widen their collection aperture for threat intelligence. Intrusion indicators are often found only after the adversary is already "inside the wire".

- **Understand the Attack:** The intrusion is just the endpoint of a longer and more complex process of planning and preparation that has come to be known as the "Cyber Kill Chain." Originally articulated by Lockheed Martin, it describes the phases of a cyber attack:
  - Reconnaissance
  - Weaponization
  - Deliver
  - Exploit
  - Install
  - Command & Control
  - Act on Objectives

- **Discerning attack activity before an intrusion requires off-network information.** Relevant data may come from specific network activity, global cyber activity, organizational policy and action, industry/sector trends, or from geopolitical events. It can be open source, proprietary, or classified. What matters most is that it the information is timely, actionable and relevant.

- **Map Your Threat Surface:** Each organization has its own risk profile based on the assets it possesses and the competitors or adversaries vying for their space. This combination is the organization's "threat surface." First, the organization must assess and prioritize its assets, analyzing security risks and vulnerabilities in all sections. Then, the organization can assess and characterize its adversaries and competitors, their intentions, their objectives, their methodologies and their opportunities on a continuous basis.

- **Total Alignment Needed:** Effective security requires clear priorities and alignment among the security team, as well as executive and senior management involvement. Cyber intelligence analysts can provide information about assets' exposure and vulnerability, but ultimately, prioritizing value, business impact (e.g., loss and disruption), and risk tolerance are executive decisions

An Evolving Discipline

Cyber intelligence continues to evolve as a discipline and an area of practice. Some companies have created sophisticated capabilities, with dedicated personnel integrated across the enterprise working at strategic, operational and tactical levels. Others, however, may have no analytic capacity but serve a security function that is compartmented and gathers intelligence only from their CERT feeds. A range of vendors and firms has emerged over the past several years offering cyber intelligence solutions for companies that cannot create their own.

Cyber intelligence continues to evolve as a discipline and an area of practice.

A number of groups also continue their work to advance the science and practice of cyber intelligence. In addition to the INSA Task Force, researchers and analysts at Carnegie Mellon University's Software Engineering Institute (SEI) (http://www.sei.cmu.edu) are an active cadre of professionals seeking to shape and expand the discipline of cyber intelligence.

In 2012, the SEI team developed the Cyber Intelligence Tradecraft Project (http://sei.cmu.edu/about/organization/etc/citp.cfm) to explore best practices used within different industry sectors. Extending the Tradecraft Project, this summer, SEI launched the

Cyber Intelligence Research Consortium (http://www.sei.cmu.edu/about/organization/etc/overview.cfm), a collective of cross-sector institutions working to improve collection and analytic methodologies, technologies and practices in cyber intelligence.

Moving Toward the Cyber Intelligence Future

Most information security professionals would say that they have a risk assessment and management approach. Some even say they use "threat intelligence," but in reality, they have no systematic intelligence capability at all.

Without an inventory of requirements and a collection management process, organizations cannot focus or prioritize the cyber threat information they collect. This makes for a "noisy" stream of threat information, within which the most useful data becomes more difficult to identify. Some try to cope by subscribing to as many feeds as possible and hoping information relevant to them will appear in the mix—but that approach is profoundly inefficient.

Cyber intelligence capabilities can make any cybersecurity enterprise more proactive and effective. By understanding their threat surface and looking well beyond the network, organizations can take on an intelligence-led approach to cyber defense and make it a dynamic, ongoing part of their culture. ●

DR. RANDY BORUM *is a professor and the Coordinator for Strategy and Intelligence Studies in the School of Information and Academic Coordinator for Cybersecurity at the University of South Florida. Additionally, he developed one the first systematic, graduate-level, academic programs of study in Cyber Intelligence and serves on INSA's Cyber Intelligence Task Force.*