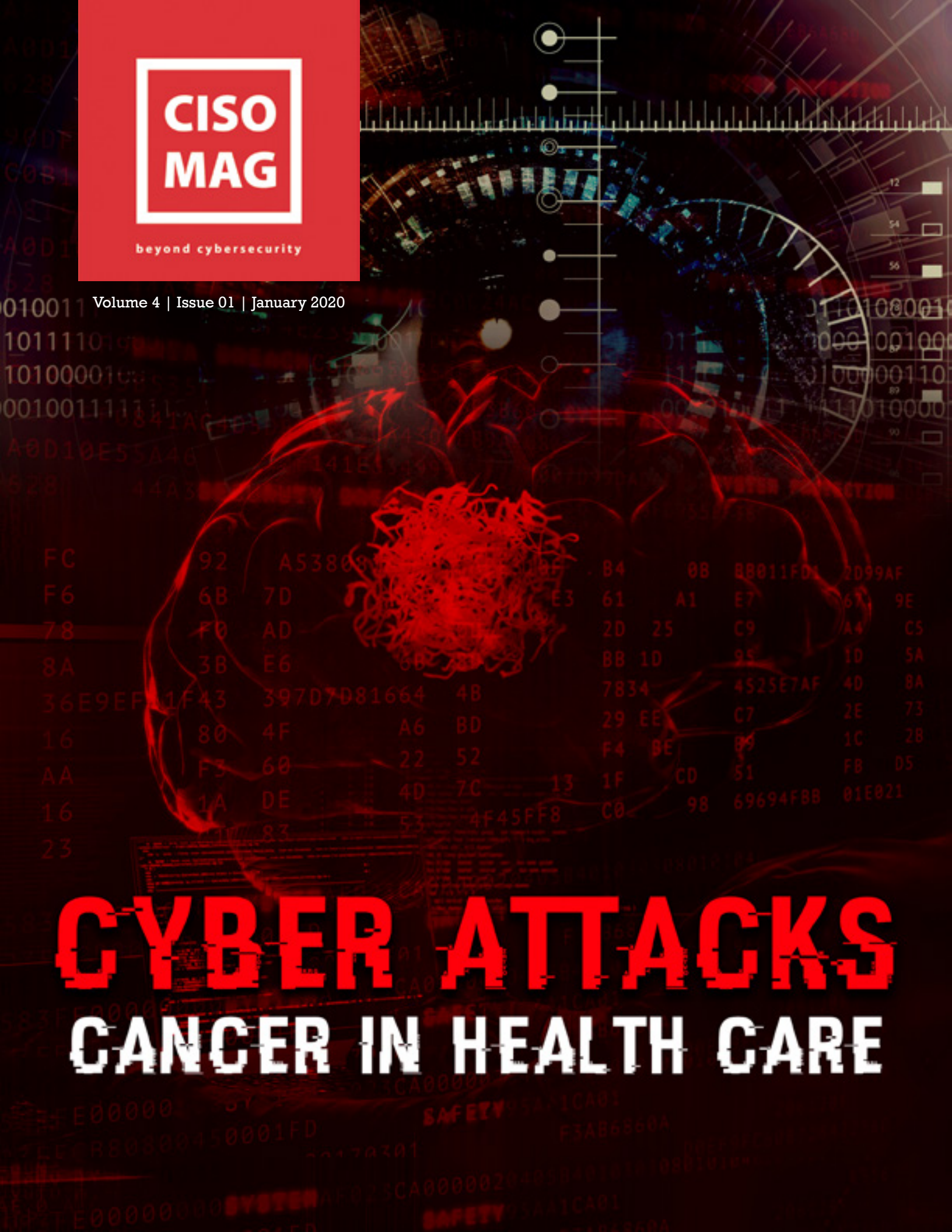
CISO MAG

beyond cybersecurity

Volume 4 | Issue 01 | January 2020



CYBER ATTACKS

CANCER IN HEALTH CARE

INDEX

VOLUME 4 ISSUE 1

EDITOR'S NOTE

We leap into 2020 with our first issue themed on Health care.

Reading a hand-written doctor's prescription usually takes a bit of effort and one wishes it was typed and printed out. The health care industry is going back to paper and pen these days, in the wake of IT system failures due to increasing ransomware attacks. Augustin Kurian reports on the impact that Ransomware made on the health care industry in recent years. His report for our cover story reaffirms the fact that Health care is the most targeted industry for hackers. For impacted health care institutions, ransomware attacks like Wannacry and others resulted in canceled outpatient appointments, elective and emergency admissions to hospitals, disrupted accident and emergency room staffing, and even deaths due to delayed treatment. And health care institutions resorted to paper-based records.

According to Beazley Breach Insights Report, health care organizations suffered the highest number of data breaches in 2018 than any sector in the U.S. economy. You can read about some headline-grabbing health care breaches on the CISO MAG website here.

In 2019, health care firms continued to be primary targets of cyber-attacks with several data breaches and ransomware attacks taking major headlines again. The financial health of the Health care industry might get even worse, with data breaches expected to cost US$ 4 billion by this time.

But why are hackers increasingly targeting health care institutions? Why is health care data (notably PHI) so valuable? Read more about it in our Cover Story section.

Tell us what you think of this issue. If you have any suggestions, comments or queries, please reach us at editorial@cisomag.com or brian.p@eccouncil.org.

Jay Bavisi
Editor-in-Chief

CISO MAG
beyond cybersecurity

Volume 4 | Issue 01
January 2020

Editorial
International Editor
Amber Pedroncelli
amber.pedroncelli@eccouncil.org

Principal Editor
Brian Pereira
brian.p@eccouncil.org

Senior Feature Writer
Augustin Kurian
augustin.k@eccouncil.org

Feature Writer
Rudra Srinivas
rudra.s@eccouncil.org

Technical Writer
Mihir Bagwe
mihir.b@eccouncil.org

Media and Design
Media Director
Saba Mohammad
saba.mohammad@eccouncil.org

Sr. Graphics Designer
Sameer Surve
sameer.s@eccouncil.org

UI/UX Designer
Rajashakher Intha
rajashakher.i@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

Senior Director, Compliance & Governance
Cherylann Vanderhide
cherylann@eccouncil.org

Deputy Business Head
Jyoti Punjabi
jyoti.punjabi@eccouncil.org

Marketing and Business Development Officer
Riddhi Chandra
riddhi.c@eccouncil.org

Digital Marketing Manager
Jiten Waghela
jiten.w@eccouncil.org

Publishing Sales Manager
Taruna Bose
taruna.b@eccouncil.org

Technology
Director of Technology
Raj Kumar Vishwakarma
rajkumar@eccouncil.org

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Brian Pereira.

VOLUME 4 ISSUE 1

BUZZ

KEYS TO A SUCCESSFUL THIRD-PARTY RISK MANAGEMENT PROCESS

Sean Friel, CEO,
Intraprise Health

5

CISO MAG | January 2020

VOLUME 4 ISSUE 1

BUZZ

The risk to health care organizations from a third-party vendor breach is clear—through August of this year alone there have been 33 breaches by a business associate/vendor totaling over 22.5 million records. That's one breach per week attributed to a third party. Organizational leaders often struggle to focus on *third-party risk management (TPRM)*—or *risk posed by third parties*, such as vendors who work with an organization and have access to sensitive patient information — despite knowing about the benefits of such a program. With a myriad of other responsibilities, focusing on the security of third parties can seem incredibly complex and time-consuming. And it is. It can take a year or more to develop an effective program, depending on the complexity of the organization and the number of third parties. But once the program is in place, personal health information (PHI) and personally identifiable information (PII) are safer and the organization has a much firmer grasp on their overall risk.

Prior to deciding to engage a partner to get a true understanding of third-party risks, it helps to understand the benefits and importance of such an undertaking. Keeping data safe, resolving security gaps—and more importantly understanding where the gaps are—and putting processes and protocols in place ultimately makes your organization stronger and helps sustain and grow your business. It's not just an IT issue to solve; third-party risk can jeopardize many areas of your hospital, health care facility, or payer organization.

Once you've decided to engage a partner to help you with your Third Party Risk Management (TPRM) program, it's time to manage expectations internally, and with your new partner, so everyone understands what's expected of each other and what the process will entail. For instance, you want the process to include every department that works with data and with third parties in an organization. A TPRM process is enterprise-wide.

You cannot rush this process. Most people who undertake the effort to build a TPRM program are surprised by how long it takes and how much work it involves, despite being educated about the process before it starts. When completed, however, they feel a huge sense of accomplishment. In effect, a solid TPRM program and process improves how organizations think and work in addition to protecting their data.

Make sure there is ownership and accountability in your organization for the TPRM program. Those stakeholders are responsible for keeping people engaged in the process and ensuring objectives are being met. They also regularly remind people why they're undertaking this huge but necessary endeavor; they are the TPRM organizational cheerleaders.

VOLUME 4 ISSUE 1

BUZZ

Utilizing external experts can help implement an effective program. Some **TPRM program implementation services** might include:

- Ensuring stakeholders across the supply chain all share a common vision and goals
- Documenting current and optimal workflows and processes so everyone involved knows what they need to achieve
- Evaluating and implementing optimized TPRM services such as assessing and revising current state workflows and processes

Here are some milestones that a good TPRM process will employ (keep in mind, each partner will offer various services, but it's important to understand what the process might include):

- Request an Assessment – Who is responsible for ensuring requests are made when needed?
- Know the potential risk a third-party could pose before starting the assessment (often called "tiering")
- Develop a solid, thoughtful and customized questionnaire based on the potential risk
- Collect evidence to validate the questionnaire responses
- Interview key vendor personnel to ensure they understand and follow a good security program
- Distill and compile the gathered information into a consumable report for decision makers
- Log and track any identified risks, regardless of severity

A good **software platform** can help to facilitate the entire process and might include:

- **Configuring TPRM workflows and dashboards**
- **Providing access to third parties who will be active participants in the process**
- **Enabling process workflow**
- **Collecting evidence and questionnaire responses**
- **Risk logging and tracking of remediation**

A health care organization's data is a vital asset that needs to be protected. Make sure the people who help you safeguard it are security-minded experts.

About the Author

Sean Friel, CEO of Intraprise Health, has dedicated his 35-year career to helping health care organizations implement technology that improves their operations and patient care. He is recognized throughout the industry for his ability to build customer focused teams that have received industry-leading customer satisfaction scores.

Most recently, Sean led rapid growth at private equity backed leading Health Information Technology companies such a Vitalhe and Lightning Bolt Solutions. As National Vice President of U.S. Sales for Siemens' Health care IT division, his team drove sales to more than US$1 billion. Prior to his 13 years at Siemens, Sean played an instrumental role in the success of Shared Medical Systems (SMS), an early leader in automating hospital systems.

Disclaimer: CISO MAG did not evaluate the advertised/mentioned product, service, or company, nor does it endorse any of the claims made by the advertisement/writer. The facts, opinions, and language in the article do not reflect the views of CISO MAG and CISO MAG does not assume any responsibility or liability for the same.