You’ve got a variety of users.

We’ve got a variety of authentication factors.

What’s Your DigitalPersona®?

Try DigitalPersona for free and discover the difference.
crossmatch.com/dpdifference
Thank You to the Executive Contributor Panel

Tarvi Schreider  
Chief Cybersecurity Strategist and Author  
Prescriptive RiskSolutions, LLC

Renee Brown Small  
CEO, Cyber Human Capital, and Author, Magnetic Hiring

Chris Roberts  
Chief of Adversarial Research and Engineering  
LARES Consulting

Raymond Teo  
Senior Vice President, Business Development, APAC  
NTT Security

Souti Dutta  
Lead Threat Analyst - SOC Services, Paladion

Aseem Ahmed  
Sr. Product Manager - Cloud Security, Akamai Technologies

Bhaskar Agasty  
Country Manager, Ixia

Nitin Kumar  
CM&A, CMC, Senior Managing Director - Technology, Media & Telecom, FTI Consulting

Richard Seiersen  
SVP & Chief Information Security Officer, LendingClub

Agnidipta Sarkar  
Global Information Risk & Continuity Officer  
DXC Technology

Jason Bloomberg  
President, Intellyx

Deepak Makhshwari  
Director of Government Affairs in India & ASEAN for Symantec

Lee Carsten  
Vice President, Client Executive, Stroz Friedberg

Sebastian Hess  
Cyber Risk Executive, AIG

Craig Moss  
COO, CREATE Compliance

Steve Duhin  
Managing Director, Information Security Forum

Jay Bavisi  
Editor-in-Chief

dt We have turned one!

On July 14, 2017, we launched CISO MAG with a vision to provide unbiased and useful information to information security professionals working in critical sectors to help them prevent, respond to, and counter security challenges. It has been a year of anxiety, long hours, and sleepless nights. But it has all been worth it.

Over the last year, CISO MAG has been able to reach 50,000 readers across 100 countries. We have interviewed over 50 security leaders and built a solid community of C-level executives in the information security domain. We have become a voice in the industry.

I would like to take this opportunity to acknowledge the contributions made by our Editorial Advisory Board, Executive Contributor Panel, and the hard working professional staff of CISO MAG.

Last but not the least, I would like to thank the readers of CISO MAG for your interest. It is your continued feedback that has enabled us to get better with every edition. Please keep sending your feedback and ideas for further improvement of our magazine at editorial@cisomag.com.

Jay Bavisi  
Editor-in-Chief

* Responsible for selection of news under PRB Act. Printed & Published by Apoorba Kumar, E-Commerce Consultants Pvt. Ltd., Editor: Rahul Arora. The publishers regret that they cannot accept liability for errors & omissions contained in this publication, however caused. The opinions & views contained in this publication are not necessarily those of the publisher. The ownership of trade marks is acknowledged. No part of this publication or any part of the contents thereof may be reproduced, stored in a retrieval system, or transmitted in any form without the permission of the publishers in writing.
Privileged and excited to be in the journey of making CISO MAG, one of the best sources of relevant and focused input on Cyber Security.

- Sunil Varkey -
Chief Information Security Officer,
Wipro Technologies

I’m very happy to be an advisor to CISO MAG. It is a well thought out, industry leading magazine that helps CISOs connect, learn, and grow in their careers.

- Geoff Hancock -
Principal at Advanced Cybersecurity Group

Honored and proud to be a part of the CISO MAG advisory board. CISO MAG is a must read for every CISO, experienced or not. CISO MAG is one of the many examples how EC-Council tries to make our world more secure, a better place to live in.

- Patric J.M. Versteeg -
Chief Information Security Officer

Constant learning is required to be proficient in information security. CISO MAG embodies this approach.

- Phil Agcaoili -
Senior Vice President at U.S. Bank
and Chief Information Security Officer
at Elavon

Having been working with Rahul and the team for a while now. It is a pleasure to congratulate the magazine on its anniversary! I love the topics and the fact they push the envelope on providing topical, useful intelligence to the community. Long may that continue!!

- Chris Roberts -
Chief of Adversarial Research and Engineering at LARES Consulting

I am on the Board of Advisors and I have enjoyed working with the CISO MAG. I feel that the organization and the magazine provide an insight into the changing role of a CISO. The magazine provides both informative articles and trends. I look forward to many years with the CISO MAG.

- Betty Lambuth -
Private Consultant

CISO MAG provides me with timely and comprehensive information addressing the array of cybersecurity and related topics. CISO MAG provides - right topics, right information that are communicated efficiently. Bottom line: CISO MAG provides a strong ROI on engagement time and all other aspects.

- Marc Glasser -
Cybersecurity Consultant and Author

FROM OUR EDITORIAL ADVISORY BOARD
Getting Cybersecurity Metrics Right: Measuring Maturity versus Results

Craig Moss
COO, CREATe Compliance

BUZZ
Establishing a practical way to measure the maturity of a cybersecurity program is critical to managing risk. You can’t improve what you don’t measure. The question for many companies, however, is ‘what should we be measuring?’ The C-suite and Boards are interested in understanding the gaps in programs and whether there are business processes in place to mitigate risks. They want to know that resources are being effectively allocated and top threats, such as those from insiders and third parties, are understood and addressed. Ultimately, the key is to have a way to evaluate the effectiveness of cybersecurity investments and to make strategic adjustments based on business and cybersecurity risk tolerance.

In a 2016 poll of 200 CEOs conducted by cybersecurity analytics company RedSeal Inc., 87% of respondents revealed a glaring need to measure the effectiveness of their cybersecurity investments. In fact, 71% of responding CEOs qualified the absence of meaningful cybersecurity metrics as a “major challenge.” A 2017 survey of 315 IT decision-makers by Dimension Research found that while 92% of respondents collected some security metrics, only 42% regularly report any metrics. The fact that metrics are being collected but not shared highlights the need for new cybersecurity metrics. Cybersecurity metrics that drive behavior to break cybersecurity out of the IT silo, improve resource allocation, assess organizational and third-party risk, and embed cybersecurity in day-to-day operations are what is truly needed to improve security.

**Defining Cybersecurity Metrics**

Edna Conway, Cisco’s Chief Security Officer, Global Value Chain, believes that cybersecurity is a part of an overall security architecture - something she refers to as “Pervasive Security.” “Security professionals need to speak the language of business - maturity and tolerance levels allow us to do that,” said Conway. Yet despite the clamoring by CEOs and boards of directors for internal security reporting, there remains a reluctance to introduce cybersecurity metrics into risk management. What underlies the reticence?

It starts with the fact that the word “metrics” means different things to different people. Each of us brings our perspective and experience to the definition. Moreover, some organizations have voiced concerns about the broad adoption of cybersecurity metrics, including:

- Governments may use metrics to establish regulatory compliance requirements.
- Companies may use metrics as standard requirements in contracting.
- Inaccurate conclusions regarding a company’s cybersecurity diligence could be drawn from certain metrics.
- Metrics may drive unfair comparisons because some industries are more attractive targets than others (e.g., financial services versus consumer products).

These concerns have thwarted the expansive use of cybersecurity metrics in general. But saying no to cybersecurity metrics is the wrong approach. The right type of metrics is needed for cybersecurity. Selecting the right metrics starts with understanding the difference between measuring cybersecurity program maturity versus measuring the resulting performance.

It is critical to make a clear distinction between the two in order to develop metrics that are valuable to an organization and its board. For improving cybersecurity, program maturity metrics are the right way to start.

Program maturity metrics look at the actions that lead to a result. They encompass the people, process, and technology elements required for an effective program. Selecting the right metrics starts with understanding the difference between measuring cybersecurity program maturity versus measuring the resulting performance.

For a practical example of the different type of metrics, let’s look at phishing. While measuring cybersecurity program maturity, we would assess the actions taken to combat phishing. This could range from having strong policies in place and effectively communicating with employees on these policies to access controls to sensitive information to a program that ensures third parties have the capacity to handle confidential information. In contrast, performance metrics measure the results of a cybersecurity program. This could range from system uptime to successfully addressing an attack of the corporate network.

For a practical example of the different type of metrics, let’s look at phishing. While measuring cybersecurity program maturity, we would assess the actions taken to combat phishing. This could range from having strong policies in place and effectively communicating with employees on these policies to access controls to sensitive information to a program that ensures third parties have the capacity to handle confidential information. In contrast, performance metrics measure the results of a cybersecurity program. This could range from system uptime to successfully addressing an attack of the corporate network.
there recurring communication to reinforce the message? Are there records? Is the organization evaluating current technology and utilizing appropriate technology to block certain phishing attempts? Is the program evaluated for effectiveness? Measuring how well the organization does these things shows the maturity of their program to reduce the risk from phishing. Performance metrics would look at the number or percent of people that clicked on a phishing email. Both metrics are useful, but the maturity metrics are a better indicator of an organization’s ability to manage cybersecurity risk.

Octavio Flores, Director of Information Technology at P&G, believes that today’s best cyber risk management practice brings three critical components together that would not be possible without maturity metrics: Information Security Strategy, Capability Maturity Model, and Enterprise Risk Management.

Flores stated, “It is all about effective risk management, to do it consistently companies need to make a strategic choice to lead and drive their security program by measuring program maturity in the areas of policy, people, process and technology. Performance metrics are also required, but program maturity focuses the company on critical capability building, coverage of those capabilities, and sustainability of performance operating those capabilities.”

There is growing acknowledgement that program maturity metrics are essential to effective cybersecurity risk management. Overall,
S U B S C R I B E  N O W
FOR COMPLETE ISSUE