

FIRST ANNIVERSARY ISSUE

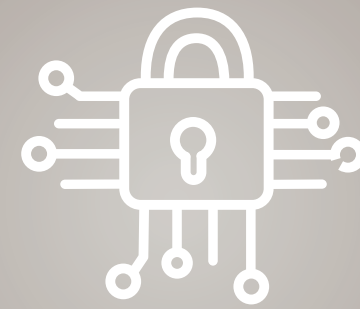
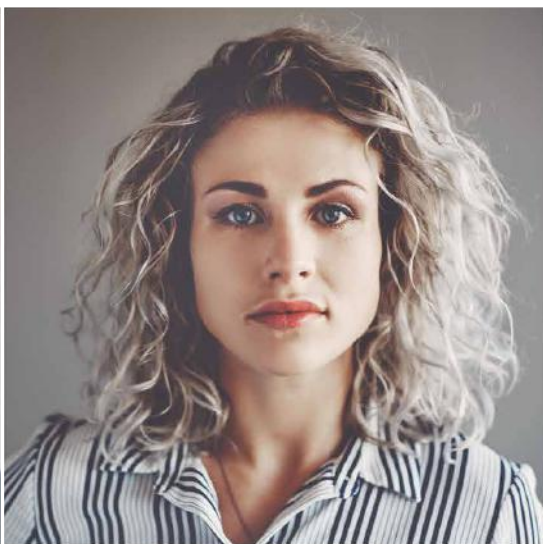


beyond cybersecurity

Volume 2 | Issue 6 | July 2018

INSIDERS THE ACHILLES HEEL





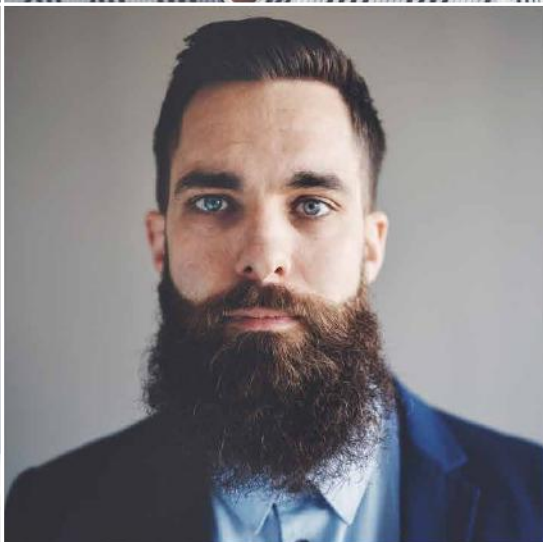
What you know.



Who you are.



What you have.



What you do.



Where you are.



When you act.

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

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



Volume 2 | Issue 6
July 2018

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

Senior Editor
Rahul Arora
rahul.arora@eccouncil.org

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

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

Designer
Jeevana Rao Jinaga
jeevana.j@eccouncil.org

Management
Executive Director
Apoorba Kumar*
apoorba@eccouncil.org

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

Marketing & Sales
General Manager
Meghana Vyas
meghana.vyas@eccouncil.org

Marketing & Business Development Officer
Pooja Saga
pooja.saga@eccouncil.org

Marketing Manager
Riddhi Chandra
riddhi.c@eccouncil.org

Sales Manager - India
Basant Das
basant.das@eccouncil.org

Sales Manager - North America
Jessica Johnson
jessica.johnson@eccouncil.org

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



Thank You to the Executive Contributor Panel

Tari 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 Agastya
Country Manager, Ixia

Nitin Kumar
CM&AA, 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 Maheshwari
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 Durbin
Managing Director, Information Security Forum

FROM OUR EDITORIAL ADVISORY BOARD



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



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



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



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



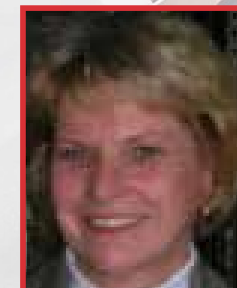
CISO MAG provides me with timely and comprehensive information addressing the array of cybersecurity and related topics. CISO MAG provides - right topics, right information that are communicated efficiently. Bottom line: CISO MAG provides a strong ROI on engagement time and all other aspects.

- Marc Glasser -
Cybersecurity Consultant and Author



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 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

INDEX



12

BUZZ

Getting Cybersecurity Metrics Right:
Measuring Maturity versus Results



24

COVER STORY

Insiders: The Achilles Heel



32

UNDER THE SPOTLIGHT

Erka Koivunen
Chief Information Security Officer
F-Secure



40

INSIGHT

Cybersecurity in an Insecure World



48

COLLABORATIONS

Infosec Partnerships



INDEX

IN THE NEWS
Top Stories from the Cybersecurity World



54



60

IN THE HOTSEAT

High-Profile Appointments in the
Cybersecurity World



64

KICKSTARTERS
Startups Making Waves in the
Cybersecurity World



17th August 2018
Singapore

Building a resilient and innovative **ASEAN**

OUR SPEAKERS



H.E. Chun Vat
Director General
Ministry of Posts and Telecommunications
Cambodia



May-Ann Lim
Managing Director
Asia Cloud Computing Association



Phannarith Ou
Director - Department of ICT Security
Ministry of Posts and Telecommunications,
Cambodia



Aman Dhingra
Associate Partner
McKinsey & Company



Malik Khan Kotadia
CEO - Finnovation Labs
Mentor - Ping An fintech accelerator



Dr. Steven Wong
President
Association for Information
Security Professionals



Tiang Lim Foo
Operating Partner
Seedplus



Vincent Loy
Managing Director
Accenture



Hock Lai Chia
President
Singapore Fintech Association,
Singapore



Jeremy Ho
Regional Director - South East Asia
Cyberbit



Joe Seunghyun Cho
Co-Founder and Chairman
Marvelstone Group



Mark Johnston
Customer Engineer - Security (JAPAC)
Google Cloud



Terry Hirsch
Chief Executive Officer
Security Weaver



Josephine Romero
Senior Adviser to the Philippines' Presidential
Adviser (Minister level) - Entrepreneurship
and Chairman
ASEAN Business Advisory Council (ASEAN
BAC) Philippines



Rohit Arora
APAC Head of Cyber Security & Networks
Citi



Ngo Quang Huy
Deputy Director General
Vietnam Computer Emergency Response
Team (VNCERT), Ministry of Information and
Communications, Vietnam



Dr. Rudi Lumanto
Chairman
Indonesia Security Incident Response Team on
Internet Infrastructure, Indonesia



Anson Zeall
Chairman
ACCESS - Singapore's Cryptocurrency and
Blockchain Industry Association



Zurkarnain Mohd Yasin
Chief Officer - Network Security and
Enforcement Sector
Malaysian Communications and
Multimedia Commission



Brig General Nicolas D. Ojeda JR
Councillor - Philippines
ASEAN Chief Information Officer Association



Prof. Lam Kwok Yan
Professor of Computer Science,
School of Computer Science and Engineering
Nanyang Technological University



Paolo Eugenio J. Baltao
Senior Vice President - EON Banking Group
Union Bank of the Philippines

EC-Council

Contact

Marketing Manager
Rakesh Acharya
rakesh.acharya@eccouncil.org
+91-79778-28905

OUR PARTNERS

Platinum Partner



Diamond Partner



Gold Partner



Silver Partners



Bronze Partner



Startup Partner



Supporting Partner



Supporting Associations



Education Partner



Exclusive Media Partner



TV Partners



Media Partners



Getting Cybersecurity Metrics Right: Measuring Maturity versus Results

Craig Moss
COO, CREATE Compliance

CASHFLOW STATEMENT

| | |
|-------------------|---------------|
| OPERATIONS | 6,554,024.00 |
| NOT SALES | 3,420,563.00 |
| INVESTMENT | 4,764,764.00 |
| EXPENSES | 1,550,452.00 |
| Development | 8,237,686.00 |
| Marketing expense | 2,679,500.00 |
| Parkings | 500,779.00 |
| NET INCOME | 57,677,812.00 |

| | |
|------|----------|
| CTMX | ▲ +98.0% |
| CST0 | ▼ -0.05% |
| FTR | ▼ -20.0% |
| CHK | ▲ +50.0% |
| AVIO | ▼ -10.0% |
| DEX | ▼ -30.0% |
| NKY | ▲ +65.0% |
| THLD | ▲ +55.0% |
| OLP | ▼ -15.0% |
| JIB | ▼ -25.0% |

STOCK MARKET REPORT

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, 72% 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. 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 communicate the phishing policies and procedures to the workforce. Is the communication part of a repeatable process? Does it routinely include new employees and contractors? Is

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,



maturity metrics are embraced by senior management and the board because they are familiar with them from many other business process improvement programs. Maturity metrics provide further confidence in the organization's capabilities to control and meet its cybersecurity risks. As a principle, higher maturity directly correlates with lower risk, better response, and better management of incidents and events.

Using Metrics to Build a Case for Additional Resources

Maturity metrics help to build cybersecurity out of the IT silo and embed it into the organization's operations. From a business and financial management standpoint, a CISO can articulate the security strategy, maturity goals, and required investments to senior management and the board. On the other side, senior management and the board can set clear and measured program maturity accountability for the CISO and expectations for the cybersecurity program.

In March 2018, the California Department of Technology released the California Cybersecurity Maturity Metrics as a further advisory measure. The California Cybersecurity Maturity Metrics are based on a customized combination of controls including those contained in the U.S. National Institute of Standards and Technology's Cybersecurity Framework (the "NIST Framework") to assess

the state's 180 entities on their program maturity in assessing the risks. California Chief Information Security Officer Steve Latham highlighted the benefits of maturity metrics in the *Wall Street Journal* on March 30, 2018, "Governments and the government's efforts are increasingly frustrated because they're getting more requests for information and resources and people for security but they have no way of assessing whether any of that works. They were unable to comprehensively look at one organization compared to another in terms of risk. This will allow folks to prioritize resources and provide resources to entities that are looking and get them up to speed."

The State of California is not alone in grappling for a way to measure cybersecurity-related risks. Based on feedback from a group of 30 large companies and associations that came together to advance the use of the NIST Framework, they learned that companies are challenged in trying to find effective and practical ways to evaluate the cybersecurity program inside their organization and those of their third parties. Increasingly, cybersecurity risk is being used as a key criterion for selecting the third parties with whom a company will partner or from whom they will acquire products or services. Yet, it has been difficult to find a available way to assess and compare the risk posed by diverse third parties.

Measuring program maturity is an effective method to assess the risk posed by third parties. It is

**SUBSCRIBE NOW
FOR COMPLETE ISSUE**