

# USING SECURITY METRICS TO DRIVE ACTION IN ASIA PACIFIC

22 Experts Share How to Communicate  
Security Program Effectiveness to  
Upper Management

Sponsored by:



# TABLE OF CONTENTS



## BRUCE HAEFELE

GENERAL MANAGER OF TECHNOLOGY,  
HEALTHDIRECT AUSTRALIA  
Compliance Is Not the Most Effective Way to  
Evaluate Security  
Pg 7



## AANCHAL GUPTA

CISO, SKYPE  
MICROSOFT  
With Security Metrics, Every Picture Tells a Story  
Pg 11



## SONG ZHANG

DIRECTOR, CISO  
HUATAI SECURITIES  
Meaningful Security Metrics Depend on Good  
Threat Intelligence  
Pg 14



## JOSEPH JAMHOUR

GROUP GENERAL MANAGER OF ARCHITECTURE AND  
SOFTWARE DEVELOPMENT,  
FUJI XEROX DOCUMENT MANAGEMENT SOLUTIONS  
Communicating Threats and Vulnerabilities to the Business  
Pg 17



## PAN CHANG

IT DIRECTOR,  
NEW YORK UNIVERSITY SHANGHAI  
University Networks Benefit from High Standards  
and Constant Monitoring  
Pg 20



## PETER MACARTHUR-KING

GENERAL MANAGER OF SECURITY AND RISK,  
SAI GLOBAL  
Use Metrics to Reveal Your Value for Money Spent  
Pg 26



## DELZAD MIRZA

HEAD, INFORMATION SECURITY  
AND COMPLIANCE,  
TATA TECHNOLOGIES  
When Evaluating Strengths and Vulnerabilities,  
Look to Your Key People  
Pg 29



## BRETT KNUTH

INFORMATION TECHNOLOGY  
SECURITY ADVISER,  
HEALTHDIRECT  
You Must Show the Importance of an Issue  
to the Business  
Pg 32



## PIETER VAN DER MERWE

CISO,  
WOOLWORTH'S GROUP  
Demonstrate Competency and Coverage,  
Without Security-Speak  
Pg 35



## ROSS SHERWIN DE CLARO

SENIOR INFORMATION SECURITY OFFICER,  
PHILIPPINE AMUSEMENT AND GAMING  
CORPORATION  
Great Security Builds on a Foundation of  
Government and Industry Standards  
Pg 38

# FOREWORD

Today's cybersecurity challenges are more complex than ever before. Technologies like Development Containers, Cloud, BYOD, and BYOA have greatly complicated the security team's ability to understand all of the potential IT attack surface. And while you may have the budget dollars to invest in new cyber technologies, the size and workload of your security team is a key gating issue. The core foundation of a successful cybersecurity program requires that you understand all of the IT assets operating against your environment, both inside and outside of your network, identify and remediate vulnerabilities, and continuously assess and measure risk.

Although organizations are investing more of their IT budget on cybersecurity technologies, high-impact breaches continue to make headlines. As a result, senior business executives and board members are asking security teams tough questions about the effectiveness of their security controls—and how they are measuring, getting control of, and reporting on cyber risk.

At Tenable, we partnered with the team at Mighty Guides to ask senior security industry leaders the following questions: "Your CEO calls and asks, 'How exposed are we, and how secure is our organization?' What strategies and metrics do you use to answer?" We compiled their responses into this e-book—giving you useful insights from your peers on how they answer these tough questions—so that you can be prepared when asked yourself.

While every organization is different and has its own unique challenges and constraints, CISOs must deliver answers that are metrics driven, benchmarked to industry best practices and standards, defensible and approximate reality.

We hope you find this e-book useful in helping you develop and communicate security metrics in your own organization. And in follow-on parts of this series, we will share with you additional market research that we know you will find compelling and useful when communicating the effectiveness of your cybersecurity program to your C-suite and Boards.



**Amit Yoran**

Chairman and Chief Executive Officer



## About Tenable

Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. Tenable's customers range from Fortune Global 500 companies, to the U.S. Department of Defense, to mid-sized and small businesses in all sectors, including finance, government, healthcare, higher education, retail and energy. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring. For more information, [please visit tenable.com](https://tenable.com).

# INTRODUCTION

As the challenge of securing digital assets grows, the challenge of quantifying an organization's security posture is also growing. This is due in part to the added layers of protection needed to secure IT infrastructures that have no perimeter, and the sheer quantities of data generated by new security technologies. It is further complicated, especially for global companies, by regional differences in security practices, standards, and regulatory environments.

In order to better understand how organizations operating in the Asia-Pacific region use metrics to describe their security posture, we decided to ask them. With Tenable's generous support, we posed this question to a number of security experts:

## ***Your CEO calls you in and asks 'Just how secure are we?' What strategies and metrics would you use to answer that question?***

For this e-book we spoke to a global audience, including security professionals from the Philippines, Australia, China and India. We found that everyone faces many of the same threats. However, different regulatory environments affect how companies think about and measure their security postures. One thing that is clearly evident from these essays is that security practices, and the metrics used to measure them, are changing, maturing, and adapting in response to a rapidly evolving risk landscape.

I believe this e-book offers valuable insights to any security executive, but especially for those operating exclusively or partially in the APAC region.



All the best,  
**David Rogelberg**  
Publisher



Mighty Guides make you stronger.

These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of advice in this guide sits right next to the contributor's name, biography, and links so that you can learn more about their work. This background information gives you the proper context for each expert's independent perspective.

Credible advice from top experts helps you make strong decisions. Strong decisions make you mighty.

© 2017 Mighty Guides, Inc. | 62 Nassau Drive | Great Neck, NY 11021 | 516-360-2622 | [www.mightyguides.com](http://www.mightyguides.com)



# SECURITY METRICS FOR THREAT MANAGEMENT

---



**BRUCE HAEFELE**  
GENERAL MANAGER OF TECHNOLOGY,  
HEALTHDIRECT AUSTRALIA  
Compliance Is Not the Most Effective Way to  
Evaluate Security  
Pg 7



**AANCHAL GUPTA**  
CISO, SKYPE  
MICROSOFT  
With Security Metrics, Every Picture Tells a Story  
Pg 11



**SONG ZHANG**  
DIRECTOR, CISO  
HUATAI SECURITIES  
Meaningful Security Metrics Depend on Good  
Threat Intelligence  
Pg 14



**JOSEPH JAMHOUR**  
GROUP GENERAL MANAGER OF ARCHITECTURE  
AND SOFTWARE DEVELOPMENT,  
FUJI XEROX DOCUMENT MANAGEMENT  
SOLUTIONS  
Communicating Threats and Vulnerabilities  
to the Business  
Pg 17



**PAN CHANG**  
IT DIRECTOR,  
NEW YORK UNIVERSITY SHANGHAI  
University Networks Benefit from High Standards  
and Constant Monitoring  
Pg 20



*We are vigilant in monitoring and enforcing that our security posture is being maintained as well as continuously looking for opportunities to improve our security stance. I would stay away from hard metrics e.g. Firewall block statistics and IPS metrics, and focus on a risk and risk mitigation based conversation as this is in line with the language that the board speaks.*



Twitter

**RICHARD TIMBOL**

ISSM/CISO, Top 10 Global Law Firm

# COMPLIANCE IS NOT THE MOST EFFECTIVE WAY TO EVALUATE SECURITY



**BRUCE  
HAEFELE**

**General Manager of  
Technology,  
Healthdirect Australia**

As the general manager of technology for Healthdirect Australia, Bruce Haefele leads and executes the vision and strategy for technology innovation, platform service, directory services, and security. His teams face today's challenges of agility and speed in a high-risk, high-compliance environment that can be addressed only by integrating security into everything they do. Haefele is passionate about applying technology to make a difference in improving social outcomes, and loves being an agitator for change.



Twitter | Website | LinkedIn



Much of his recent career has been serving companies in the healthcare field. As a result, Bruce Haefele, general manager of technology for Healthdirect Australia, is particularly sensitive to security and has a unique approach to assessing readiness at any given point. "We tend to talk a lot about compliance," says Haefele, "but compliance doesn't really tell you how secure you are. It just tells you whether you can meet standards in some circumstances. I think that it is time to give people a sense of just how exposed we might be. It is a moving target, so you need things that move along with that target."

"Compliance is the minimum point," Haefele believes. "We have to be compliant. It is federally mandated. Obviously, becoming compliant forces you to mature your security practices to a point, but if people think that is what's being safe or being invulnerable, they're just kidding themselves. There is generally better recognition, certainly among security professionals and increasingly at the executive and board level, that being breached is a case of when, not if. It is just as important to have security response strategies and be able to handle security incidents."

*“ Obviously, becoming compliant forces you to mature your security practices to a point, but if people think that is what's being safe or being invulnerable, they're just kidding themselves. ”*

## KEY LESSONS

- 1 Compliance with various government or third-party regulations is merely a start in building a meaningful security wall.
- 2 Leverage a maturity matrix model which proposes a security maturity score.



# COMPLIANCE IS NOT THE MOST EFFECTIVE WAY TO EVALUATE SECURITY

As his firm operates under the Information Security Manual (the equivalent of FedRAMP in Australia, administered by the Australian Signals Directorate), four mandatory areas need to be addressed: application whitelisting, patching applications, patching the operating system and minimizing administrative privileges. These four areas are known as the [Top 4 controls](#), which account for the most critical attack vectors. Each of these tells an important story, says Haeefele, but not a complete one. That comes only from the compilation of several metrics and reports and varies depending on who's looking at the data.

“The interesting one among that group” says Haeefele, “is probably the patching side because it shows both exposure and the effectiveness of your processes. I might look at reported external penetration tests as revealed over time, or I might look at the vulnerability rating. We scan every night. I look at how those vulnerability rates are moving over time and then divide it by category of risk—from critical to high to medium and so on. We also look at the daily vulnerability count over time.”

Another area Haeefele believes merits consideration is the maturity matrix model, which proposes a security maturity score. A score of 1 means compliance minimum, 2 is industry baseline, 3 is industry best practice, and 4 is best in class. “That gives a more qualitative measure of where security feels it sits relative to its peers,” says Haeefele.

“These benchmark-type statistics are important for executives and boards in particular,” says Haeefele. “Another interesting metric is the top-three security risk exposures, the actions that would remediate those, and the residual risk that would follow remediation. Again, this metric shows the priority for investments in security, and if you rate that visibility, you can often get the momentum of the board or the exec behind actually effecting those changes.”

“

*What executives and boards really want to know are: What is my risk exposure here? How is that affecting our business? What are the options to reduce that risk exposure? Are our processes and practices working? Do we have sufficient funding to actually get to the security posture we would like? ”*





# COMPLIANCE IS NOT THE MOST EFFECTIVE WAY TO EVALUATE SECURITY

Haefele also believes that a security staff engagement score is useful. “We do a staff engagement survey every year,” he says, “and it is quite detailed and actually benchmarks different groups against each other. If your security staff are engaged and feeling like they can do their job, that is probably an indication that you have health in your security posture. Anecdotally, we also ask the general staff about security to determine whether they feel security aware, and whether they feel there is a balance between security and productivity.”

In Australia, company directors can be held personally liable for security breaches. As a result, Haefele feels that security awareness is high there. “What executives and boards really want to know about,” he says, “are: What is my risk exposure here? How is that affecting our business? What are the options to reduce that risk exposure? Are our processes and practices working? Do we have sufficient funding to actually get to the security posture we would like?”

“Ultimately, we would all like to get to more predictive analytics, which can predict where vulnerabilities are starting to be exposed,” says Haefele. “But we are not there yet.”



*There is no 'simple' / one-size-fits-all method to answering "Just how secure are we?" - as in all things cyber 'it depends.'*

- The security leadership must develop a 'CISO Scorecard' that assesses the many security/ risk measures that best embody a risk based security strategy approach, distilling the many operational and strategic metrics into those that matter to the BoD.*
- Any CISO scorecard is part art and science, whereas there is no shortage of authoritative sources on 'what' to measure; the art is then selecting those metrics that show both risk reduction and enhancing the business success and competitive advantage.*



  
LinkedIn

## MIKE DAVIS

Director, IT Security (CISO) at American Bureau of Shipping

# WITH SECURITY METRICS, EVERY PICTURE TELLS A STORY



**AANCHAL  
GUPTA**  
CISO, Skype,  
Microsoft

Aanchal Gupta leads a team of experts at Microsoft in the areas of security, privacy, and compliance. She is passionate about building products that are safe, trustworthy, and accessible to everyday users. Prior to joining Microsoft, Aanchal led Yahoo!'s Global Identity team, contributing to various authentication and authorization open standards such as OpenID and OAuth. She has more than two decades of experience leading large, distributed development teams developing global software used by millions.



Twitter | Website | LinkedIn



Aanchal Gupta empathizes with C-suite executives' need to get to the point of any discussion. As chief information security officer (CISO) for Skype and Skype for Business, she appreciates terseness from her own team.

When an executive asks her for an enterprise security update, she shows the same courtesy. That attitude helps guide her selection of metrics to illustrate business-risk assessments to senior leaders. Examples of those metrics include:

- **Externally reported security incidents.** Because Skype is a public-facing, Microsoft-owned communications platform, external researchers do a lot of testing on Skype. "Anything that is reported is taken very seriously. We track these issues closely," Gupta says. She graphs incidents over time, she states, to help leadership understand whether Skype is addressing these potential vulnerabilities. She also tracks the mean time to resolve each issue. If, over time, both graphs do not trend downward, she notes, "Then something is wrong—we are not focusing our engineering investments in the right places."

*“ Right away you get four follow up meeting invitations from the engineering managers: ‘Can you walk my team through why we are red and how we can get to green?’ ”*

## KEY LESSONS

- 1 Tracking externally reported incidents will help you determine whether your security preparedness is trending in the right direction.
- 2 Don't try to tell the whole story verbally. A data-rich trend graph can be much more compelling and convincing than any speech.



# WITH SECURITY METRICS, EVERY PICTURE TELLS A STORY

- **Penetration testing.** Skype regularly pen-tests its own product, Gupta notes, and this metric reveals any visible gaps. “I try to categorize those gaps for our leadership team,” she adds. Skype uses Microsoft’s “STRIDE” model to categorize threats—an acronym that stands for “spoofing identity,” “tampering with data,” “repudiation threats,” “information disclosure,” “denial of service,” and “elevation of privilege.” The metric is important to senior leadership, Gupta asserts, because they know that penetration failures can be prevented with more in-depth training.
- **Engineering security maturity.** Gupta believes that when engineers understand that they’re responsible for security from the requirements phase all throughout the development process, the final product is more secure. That’s why threat modeling is required of the Skype engineering teams. She uses color-coded heat maps to track teams’ relative security-preparedness ranking graphically, she says. The best prepared fall into the green zone; the least prepared are color-coded red. This is a simple way to communicate to executives which engineering teams need “encouragement” to focus more on security. “You can see the wheels moving right away,” she comments. “You leave the executive meeting and right away you get four follow up meeting invitations from the engineering managers: ‘Can you walk my team through why we are red and how we can get to green?’”

It is important for CISOs to avoid presenting prebaked metrics to executives, Gupta cautions. If at an executive meeting you point out that the organization has several open security issues, someone will ask you to prioritize and rank them. If you reply that some of the issues you have charted have not yet been severity-ranked, leadership will not be happy.

“Don’t go to your leadership unprepared,” Gupta urges, “Your data should reflect the homework you have done.”

A final insight: a picture is worth a thousand words, especially one that illustrates your metrics in an effective and cogent way. “You may speak for an hour and nobody will believe that you have affected the problem,” Gupta contends. “But if you show leadership a trend graph, they’ll be convinced.”

“

*Don’t go to  
your leadership  
unprepared.  
Your data should  
reflect the  
homework you  
have done.*

”



*Based on our organizational risk appetite, and our own risk analysis, we are as secure as we can be within our budget, people and organizational constraints. We have addressed the top 10 most harmful cyber risks to the business using a mixture of approaches, are continuing to monitor those top 10 risks and approaches and have rehearsed plans to help us deal with new or unexpected risks.*



Twitter



Website



LinkedIn

# ADRIAN DAVIS

Managing Director EMEA, (ISC)<sup>2</sup>





**SONG  
ZHANG**  
Director, CISO,  
Huatai Securities

As chief information security officer for Huatai Securities, Song Zhang advises the firm's executive leadership, business, risk management, and IT teams on protecting firm information and IT assets. Song Zhang manages the enterprise cybersecurity and information risk programs, security architecture, security operations, risk and compliance, and data security investigations. His mission is to adopt a risk-based approach and international best practices to ensure the firm has positive security behaviors that protect their information assets.



Website

Song Zhang, chief information security officer at Huatai Securities, says that his team delivers a full security report to the company's top executives every month. "Our executives always have a full understanding of the level of security threats and the risk landscape of the whole organization," Song Zhang says. The monthly report uses a total-risk-level metric to describe specific cybersecurity risk levels as moderate, high, or very high. In this way, he can focus attention on vulnerable areas and quickly show progress that has been made over earlier reports.

Several factors go into determining the total risk levels, but they fall into three categories of key indicators:

- **Instances of Mature Impact.** This key indicator is made up of metrics related to actual attack instances that have an impact on the system. For example, an identified instance will include metrics such as the number of compromised systems, the number of potentially compromised systems, the number of data breaches related to internal or external fraud, and other factors. "We use these metrics to create a penetration rate index," Song Zhang says. "That metric allows us to show, with a high confidence level, what happened in the past and what may happen again."

*“ We use these metrics to create a penetration rate index. That metric allows us to show, with a high confidence level, what happened in the past and what may happen again. ”*

## KEY LESSONS

- 1 The monthly security report uses a total-risk-level metric to describe specific cybersecurity risk levels as moderate, high, or very high.
- 2 Several factors go into determining the total risk levels, but they fall into three categories of key indicators: instances of mature impact, known risk, and unknown risk.



# MEANINGFUL SECURITY METRICS DEPEND ON GOOD THREAT INTELLIGENCE

- **Known Risk.** Song Zhang's team uses Gartner's Adaptive Security Architecture to address a constantly changing risk landscape. "We assume our prevention controls may be compromised at any time by anyone." For known risk indicators, his team focuses on metrics related to time to detect and time to contain.
- **Unknown Risk.** This category focuses on key indicators that show an overall level of protection against any kind of threat. "One indicator is our next-generation threat prevention capability, which we are currently expanding from layer four to layer seven firewall protection," Song Zhang says. Another indicator is a measure of asset management coverage, which includes in-depth asset management capabilities, such as installed software/running service visibility, asset discovery and abnormal protocol traffic. "We also look at a 'build security in' factor, or BSI, which focuses on building security capability into the IT system development life cycle," Song Zhang says. "By measuring that, we can show our overall progress in strengthening the IT system." One of the most important parts of the unknown risk category is the use of threat intelligence. Song Zhang explains, "Without threat intelligence, it is difficult to analyze the huge amount of security data on a day-to-day basis." Threat intelligence is integrated into the system and used to actively seek out and intercept threats before they become breaches. Song Zhang's team uses Tenable's solution for this purpose, and they use a metric that shows how many threats have been caught by their system.

In analyzing their company's security posture, there are some traditional metrics Song Zhang's team does not consider. "We skip most traditional metrics," Song Zhang says. "For example, a traditional metric that is less important is the patching ratio or the patching alerts generated by the prevention controls, because there are too many. We get 100,000 attacks per month on an NG firewall. It's not possible to view all that data. That's why we use threat intelligence and threat-centric approach to analyze all the data and look for threat patterns and adjust priority in vulnerability management."

Compliance analytics are less important for Song Zhang's team, since cyberthreats are the main focus. Song Zhang expects he will be tracking more compliance metrics in the future when external threats are managed well and regulatory pressure increases.

“

*Without threat intelligence, it is difficult to analyze the huge amount of security data on a day-to-day basis.*

”



*If you're tracking metrics for things that aren't tied to what you're trying to achieve, you're failing. And if you're tracking metrics for things that you have no intention of ever acting on, you're also failing. The primary questions should be, 'why am I tracking this, and what do I intend to do when I get a certain result?'*



Twitter



Website



Blog



LinkedIn

# DANIEL MIESSLER

Director of Advisory Services, IOActive



## JOSEPH JAMHOUR

Group General Manager of  
Architecture and Software  
Development,  
Fuji Xerox Document  
Management Solutions

Joseph Jamhour is the group general manager of Architecture and Software Development at Fuji Xerox Document Management Solutions. Jamhour provides technology leadership for a team of professionals who design and develop innovative, robust, and secure IT solutions. Recently, Jamhour has focused on the planning and design of a cybersecurity program to elevate the security maturity level and deliver agility and continual adaptability to the ever-changing landscape. Jamhour holds an MBA and is a Certified Information Security Manager.



LinkedIn

Joseph Jamhour, group general manager of Architecture and Software Development for Fuji Xerox Document Management Solutions, says that communicating security vulnerabilities requires two perspectives. The first is an “outsider” perspective, and the second is an internal one. At the same time, organisations need to understand the resource implications of implementing a vulnerability management program and their risk appetite.

“A strong approach for IT departments is to profile the critical assets in how they are tied to organisational capability, then assess how those vulnerabilities could compromise the business. The next step focuses on risk management, which provides further context for the program in addition to driving compliance actions and outcomes,” says Jamhour.

Jamhour explains that from an “outsider” or hacker perspective, in terms of overall security infrastructure, organisations should look at the critical assets that need to be protected. The number of vulnerabilities detected on external-facing systems or systems that have had exposure to the internet clearly illustrate the businesses’ visible vulnerability position and will help to form an initial approach towards developing a vulnerability management program.

“ A strong approach for IT departments is to profile the critical assets in how they are tied to organisational capability, then assess how those vulnerabilities could compromise the business. ”

## KEY LESSONS

- 1 To reach an operational state of maturity and continuous improvement in cybersecurity management, organisations should establish a plan that focuses on governance, risk and compliance.
- 2 Establish a baseline of metrics and use those metrics to assess what is happening in your environment, and provide executive reports.



# COMMUNICATING THREATS AND VULNERABILITIES TO THE BUSINESS

“This outside perspective,” says Jamhour, “might come from an ethical hacking exercise where you’re illustrating the ease of vulnerability discovery and likelihood of compromise.”

He also says that, “generating awareness is key to reporting on an organisation’s vulnerability position. To help executives understand their position, it’s best to identify a scenario, usually relating to a product or service sold by the organisation, that resonates by highlighting the business impact in terms of financial performance or brand damage.”

IT departments must help executives understand that taking a risk-based approach can help develop the vulnerability response plan and progress to acceptable outcomes. Also, identifying risk factors helps to assess the impact on resources and can justify a review of roles and responsibilities.

## Ensuring Success

In order to fully realise organisational capability in cybersecurity management, and to reach an operational state of maturity and continuous improvement, organisations should be encouraged to establish a plan that focuses on governance, risk and compliance. That plan should be developed in consensus with senior executives and include both high risk items and quick wins while carefully ensuring timely reporting, communication and transparency. At the same time, technology teams should be adequately resourced and funded to support the agreed upon plan.

Jamhour continues, “External vulnerabilities and subsequent threats are usually easier to communicate than internal ones. The insider threat landscape and internally visible vulnerabilities are not specifically reflected within incident reporting, yet they pose a far greater risk when there is a breach.” Additionally, senior executives often do not have a clear perspective of the internal threats due to the highly technical nature of the conversation.

“

*To help executives understand their position, it’s best to identify a scenario... that resonates by highlighting the business impact in terms of financial performance or brand damage.*

”





# COMMUNICATING THREATS AND VULNERABILITIES TO THE BUSINESS

For those starting out on this security management journey, establishing a baseline of metrics is particularly important. Using those metrics to assess what is happening in your environment, and then providing executive reports, is invaluable when developing a cohesive and mature response.

Elements of a mature response typically include implementing strong data governance practices, patching regimes, user account hygiene and principles around need to know and separation. Therefore, the source data of the metrics can include detected vulnerabilities, remediated vulnerabilities, malware detections, failed logons, new account creations, deletions and privilege escalations.

Gathering that data and presenting it in an easily digestible format is key for IT departments to communicate effectively with senior executives to generate support for security programs.



*At the present time there are no major, ongoing, security incidents being reported. Several measures are in place to prevent and detect incidents in the shortest amount of time possible when a breach occurs, and the appropriate response plans have been put in place based on the sensitivity of the data on the affected systems and the importance to business operations.*



Twitter



Website



LinkedIn

# PAUL ASADOORIAN

Founder & CEO, Security Weekly



## PAN CHANG

IT Director,  
New York University  
Shanghai

Pan Chang, IT director for NYU Shanghai, is responsible for advancing technology in support of teaching, learning, research, and administration across the NYU Shanghai campus. Before joining NYU Shanghai, he served as vice CIO and IT director of Shanghai Jiaotong University School of Medicine and IT director of Shanghai Academy of Social Science. Prior to that, Pan Chang was chief of the network and system team and a senior engineer at East China Normal University.



Website

Pan Chang faces a combination of challenges in his work to secure the complex network of New York University (NYU) in China. In addition to demanding requirements from NYU's United States-based leadership, he must meet the Chinese government's standards for internet use and other security measures. Add in a population of students, faculty, and others, all of whom need various levels of network access, and you have multiple points of vulnerability.

"Our students are students of NYU, and so we must deliver the same standards and quality here as in the United States," says Pan Chang. For his team, that means constant vigilance, watching over a large network that has multiple layers of protection. To the "home team" security experts back in the United States, this tends to mean strict compliance to system-wide standards for hardware, software, firewall protection, authentication, and other measurable data points. Although Pan Chang knows that building a reliable and well-protected network is at the core of any security plan, he also sees that local realities and usage dictate a holistic look at network traffic. Consequently, threat detection and vulnerability assessment are the most important areas he and his team consider.

"We use software to look not just at possible threatening traffic coming to our network," says Pan

*“ We use software to look not just at possible threatening traffic coming to our network but increasingly at activity and patterns that third-party monitoring identifies. ”*

## KEY LESSONS

- 1 Once a secure and dependable security system is in place, the extra edge comes from intelligence—understanding host vulnerabilities, potentially weak access points, authentication issues, outside threat patterns, etc.
- 2 Any extra security edge is likely going to come from intelligence, not additional layers of protection.



Chang, “but increasingly at activity and patterns that third-party monitoring identifies. So, if a particular type of malicious hack is taking place against similar networks, we can determine whether we are at risk.” Those measures, combined with a rigid set of technical specifications, standardized software, and best practices with NYU’s American campus, provides basic defense—to a point—but with students using their own hardware and a sometimes-curious attitude about the world outside China, vulnerabilities are constant.

Pan Chang makes a clear distinction between direct threats to school servers in the United States and China, all of which are protected by multiple firewalls and strict software management, and the many avenues of access attackers can exploit through the large population of student and faculty network users. “Our biggest security threats come from email,” says Pan Chang, “and students who may visit unsafe websites.” Unlike their U.S. counterparts, NYU students in China are much more likely to access school networks through mobile devices. In fact, most student access is provided wirelessly, which is another important monitoring point for Pan Chang’s team.

Pan Chang and his U.S. counterparts allocate priority and resources in part based on the type of data they are protecting. NYU has a four-stage hierarchy of data protection:

- **Restricted data.** Data whose unauthorized access or loss could seriously or adversely affect NYU, a partner, or the public (e.g., banking and credit card data, health information).
- **Protected data.** Data with a slightly lower-level of importance than restricted data but that should be protected against general access (e.g., NYU intellectual property, human resources data, final course grades).
- **Confidential data.** All other non-public data that does not fall into the restricted or protected data classes are considered confidential.
- **Public data.** Public data has no protection, and general access is allowed.

Pan Chang and his team take every level of security seriously and realize that attackers will ultimately find the vulnerable spots and exploit them, if possible, so constant vigilance and monitoring are what allow them to sleep at night. “We depend on a customizable dashboard that we can view on our mobile devices,” he says. With best-in-class security systems in place and all the appropriate back-up and response mechanisms lined up and operating properly, any extra security edge is likely going to come from intelligence, not additional layers of protection.

“  
*We depend on  
a customizable  
dashboard that we  
can view on our  
mobile devices.*  
”



*What I'm trying to do from a strategic point of view is find those metrics that are really going to resonate with the business...Executives don't want to hear about servers, and the security analysts don't want to talk to the executives. So I guess I'm a universal translator.*



  
LinkedIn

# NIKK GILBERT

Director of Global Information Protection and Assurance,  
ConocoPhillips



# SECURITY METRICS THAT TELL A STORY TO THE BOARD

---



**PETER MACARTHUR-KING**

GENERAL MANAGER OF SECURITY AND RISK,  
SAI GLOBAL

Use Metrics to Reveal Your Value for Money Spent  
Pg 26



**DELZAD MIRZA**

HEAD, INFORMATION SECURITY  
AND COMPLIANCE,  
TATA TECHNOLOGIES

When Evaluating Strengths and Vulnerabilities,  
Look to Your Key People  
Pg 29



**BRETT KNUTH**

INFORMATION TECHNOLOGY  
SECURITY ADVISER,  
HEALTHDIRECT

You Must Show the Importance of an Issue  
to the Business  
Pg 32



**PIETER VAN DER MERWE**

CISO,  
WOOLWORTH'S GROUP

Demonstrate Competency and Coverage,  
Without Security-Speak  
Pg 35



**ROSS SHERWIN DE CLARO**



SENIOR INFORMATION SECURITY OFFICER,  
PHILIPPINE AMUSEMENT AND GAMING  
CORPORATION

Great Security Builds on a Foundation of  
Government and Industry Standards  
Pg 38



*One effective method for communicating the state of your cybersecurity to the CEO is a dashboard.*



 |   
Twitter | Website

## ROBIN "MONTANA" WILLIAMS

Senior Manager, Cybersecurity Practices & Cyber Evangelist,  
ISACA

# USE METRICS TO REVEAL YOUR VALUE FOR MONEY SPENT



## PETER MACARTHUR-KING

General Manager of  
Security and Risk,  
SAI Global

Peter Macarthur-King has 32 years of IT experience, having held positions as an academic, software developer, server and network engineer, security specialist, IT architect, and IT manager. At Fujitsu Australia, he managed the network, server, and security teams. From there, he became a corporate IT architect and finally served as a corporate IT manager. He joined SAI Global as head of infrastructure Asia-Pacific; now, Peter is general manager of SAI's security and risk.



Website | LinkedIn



SAI Global hosts many Software as a Service products for hundreds of thousands of customers around the world. The company maintains hosting environments that adhere to the ISO 27001 standard for information security. As general manager of security and risk, Peter Macarthur-King manages all IT and information security for the entire organisation. In this capacity, he sets policies and standards, monitors compliance, and runs internal vulnerability assessment systems. He also spends a lot of time addressing matters of security with executives in the company, and he works through numerous security audits required by corporate clients. This experience has given him plenty of opportunity to zero in on metrics that give an accurate picture of the organisation's security posture as well as metrics that are not so helpful.

“What I try to do is show progress toward a goal,” says Macarthur-King. “The metrics I put out show that we are improving over time, or that we are not doing so well in a particular area and need to improve.” Macarthur-King likes trend metrics that link to policies and practices. For instance, metrics related to staff training are useful because one of the weakest security links in any organisation is staff. “I like to see how many staff have been trained and with what courses, how many successfully completed the training, and then tie those metrics to incident trend metrics,” Macarthur-King says.

“ *The metrics I put out show that we are improving over time, or that we are not doing so well in a particular area and need to improve.* ”

### KEY LESSONS

- 1 For the executive audience, you want metrics that show the value they are getting for the money they are spending on security.
- 2 Showing a ratio of blocking events in relation to actual incidents helps drive home the importance and value of the security investment.



# USE METRICS TO REVEAL YOUR VALUE FOR MONEY SPENT

Another useful metric relates to patching and how the company stands in applying critical patches. “I created a dashboard that shows critical patches needed by region,” Macarthur-King says. “It gives a running count, and it looks back six months. You can see at a glance the current count of outstanding patches by region, how that compares with recent months, and how it’s trending.”

For the executive audience, you want metrics that show the value they are getting for the money they are spending on security. Some metrics are not helpful in this regard. For example, incident metrics can be misleading. Macarthur-King says, “In our case, we have few incidents. If I report month after month that we had no incidents, they stop taking notice of the fact that there are no incidents. They think, ‘What are we spending all this money on?’” Macarthur-King presents incident data differently, preferring to move outside the wall to show a ratio of attacks to incidents. By showing ratio metrics around the number of emails that were quarantined; the number of emails that got sandboxed, unpacked, and identified as having malicious payload; or the number of first hits that came through before they were re-sandboxed and then squashed, Macarthur-King can show event numbers in relation to actual incidents to help drive home the importance and value of the security investment.

Risk metrics are also important to the executive-level audience. “I am trying to get some access control tools to manage elevated rights, so I need to show that risk at the executive level and then when I start asking for tools, tie those risks back to the tools needed to address the risk.”

“The executives question the cost and the effort,” Macarthur-King says. “I think it is important for executives to understand the threats that are actively being used against them, and the capability of the systems we are implementing to block them.” It is an approach to security metrics that stresses the potential rather than the kinetic. “What is the buildup on the outside of the wall? If the dike breaks, what is going to happen to us? Showing that delta is critical to continuing to get a budget.”

“  
*It is important for executives to understand the threats that are actively being used against them, and the capability of the systems we are implementing to block them.*”



*You need to have metrics and messages across security that are specific, measurable, attainable, relevant, and time-bound. If you don't, you are going to lose your audience.*



## OMKHAR ARASARATNAM

CTO of CISO and Global Head of Strategy, Architecture and Engineering, Deutsche Bank



## DELZAD MIRZA

Head, Information Security  
& Compliance,  
Tata Technologies

Delzad Mirza has been in charge of cybersecurity and business risks at Tata Technologies for the past six years. A professional with more than 12 years of experience, he focuses on information security, risk management, vulnerability assessments, audits, software licensing, compliance, and anti-piracy. As global CISO, he manages information security and compliance teams in support of 8,500 users across more than 13 countries.



LinkedIn

When Delzad Mirza recently made a presentation to his company’s board on the topic of security posture, he was blunt. “What I told them,” he says, “is that every organization has a good security plan until they get punched in the face. What, then, do we do? It’s not a question of *whether* you’re going to get hacked but *when*.” Against this backdrop of inevitability, Mirza and his team work feverishly to keep potential threats at bay and look to a variety of compliance standards, policies and procedures, and employee training and development as potential measures of success. It is that last component—employee training and development—that is currently top-of-mind for Mirza as he steps back and looks at how breaches and attacks typically occur.

“One of the prime metrics we look at regularly comes from monitoring privilege use in the company,” he says. “Who has administrator privileges, who doesn’t have administrator privileges, because if you look at the recent malware trends—and we’ve done a couple of assessments—these attacks try to identify accounts that have privileged access. These attacks always exploit people more than technology.”

“ *Every organization has a good security plan until they get punched in the face.* ”

## KEY LESSONS

- 1 Employees who have network administrative privileges are often the entry point for malicious hackers, so monitoring and training at that level are essential.
- 2 Keeping everyone hyper-aware of pending threats is essential.



## WHEN EVALUATING STRENGTHS AND VULNERABILITIES, LOOK TO YOUR KEY PEOPLE

So, Mirza works hard to build employee awareness, which his team monitors regularly. “New people who are joining the company,” says Mirza, “go through an hour-long training session during which we ask them to take a quiz of about 25 questions. Then, we monitor those employees monthly.” This awareness training and monitoring cover basic information security topics designed to help employees identify vulnerabilities and behavior that might lead to problems as well as to identify potential internal threats.

“After someone goes through the training,” says Mirza, “we send out frequent mailers, kind of an awareness mailer/poster. We send it out to all our employees, and then about every six months, we have a session with the marketing team—a town hall-type meeting during which we pick people out and ask, ‘What would you do if x, y, or z happened? Whom would you contact? What would you do?’”

The same concern for how internal behavior can expose organizations to risk has led to Mirza’s team adopting a strict no-tolerance policy toward software piracy. This is an appropriate posture for a company that builds quite a bit of proprietary code, and partners with the world’s most successful automotive manufacturers to deploy effective vehicle programmes and deliver discrete work packages to complete end-to-end design and development. It is also a way to prevent unauthorized or unapproved software entering the organization—software that can become a way in for those seeking to do damage or compromise data.

“We’ve created scripts that identify key generators, license files, serial keys, and other licensing data stored on our end-user systems,” says Mirza, “and then we track the results monthly. If we find anything, that user is taken to task, including having their external hard drive blocked, privileges revoked, etc.”

When the board asks Mirza how the company is doing security-wise, he has two key areas to point to. Externally, there are a host of strict compliance standards, such as ISO 27001, and a track record of excellence. Just as importantly, Mirza and his team have the internal side covered, as well, with its unique internal training and monthly monitoring of employee awareness.

“

*One of the prime metrics we look at regularly comes from monitoring privilege use in the company. Who has administrator privileges, who doesn’t have administrator privileges, because if you look at the recent malware trends—and we’ve done a couple of assessments—these attacks try to identify accounts that have privileged access.*

”





*By comparing your assets, controls, and vulnerabilities, you are able to have a better view of your security posture. And with that visibility, you can make the decisions you need to make, such as what you're willing to spend to align your security posture to your risk appetite.*



Twitter

# TROELS OERTING

Group Chief Information Security Officer, Barclays

# YOU MUST SHOW THE IMPORTANCE OF AN ISSUE TO THE BUSINESS



**BRETT  
KNUTH**

**Information Technology  
Security Adviser,  
Healthdirect**

Brett Knuth is a results-driven IT executive with expertise in information security, risk, and compliance. He has cross-industry experience in senior management positions, delivering security services to such organisations as IBM, Westpac, and the Australian government. Brett's technical knowledge is clear through his experience managing teams both local and remote coupled with a track record of delivering superior customer service. He operates at all organisational levels and is a trusted adviser to IT teams and lines of business alike.



Website | LinkedIn



The way an organisation uses security metrics to evaluate its security posture varies with the type of organisation and the kinds of data it must protect. This point is well illustrated by Healthdirect Australia, a government-owned and -funded company that provides free health care information portal services to consumers.

Healthdirect does not capture a lot of sensitive data, but it still must comply with security controls described in the Australian Signals Directorate (ASD) information security manual (ISM). As Brett Knuth, certified information security manager for Healthdirect explains, “We do not store a lot of high-value data. Our systems are all classified as unclassified systems, but because we are a government organisation, we are required to conform to something like 932 controls from the ISM.”

As is true for many organisations in Australia, Healthdirect relies on a third party for penetration testing, and an assessor from the Information Security Registered Assessors Program (IRAP) must audit that testing. “We have the report independently audited by an IRAP assessor. Both the IRAP assessor and ASD get the Pen Test report as it is,” Knuth says.

“ *Every night, we scan the production environment internally and externally. We limit our exposure by making sure those internal and external vulnerabilities are addressed as quickly as humanly possible.* ”

## KEY LESSONS

- 1** In presenting the security posture to business executives and the board, whether for purposes of addressing a particular issue or justifying a budget allocation, avoid technical details.
- 2** Explain the risk, the likelihood of the risk, and the risk rating based on our risk framework.



# YOU MUST SHOW THE IMPORTANCE OF AN ISSUE TO THE BUSINESS

If the testing finds noncompliance or unpremeditated risks, Healthdirect is called to account. If an organisation is found to be more vulnerable than it should be, or it is not adequately conforming to ISM regulations, the ASD may give that organisation 30, 60, or 90 days to remediate. “Or they can require you to switch off the solution,” Knuth says. “They can tell you that you can’t go live because your solution is too vulnerable and the risk of brand and reputation damage to yourselves and to the agency is too great.”

The IMS specifies risk-based controls that fall into two categories: *Musts* (Must and Must Not) and *Shoulds* (Should and Should Not). *Musts* represent higher risk controls and *shoulds* are medium to low-risk controls. “If we miss on the ‘Must’ controls, we have to explain why to the security director of ASD and, in some cases, to other agencies that also have oversight,” says Knuth.

For a solution to go live and be in production, it has already been independently Pen tested, certified, and accredited to go live. Knuth says, “From then on, I base my assessment on the vulnerability report from Tenable SecurityCenter. Every night, we scan the production environment internally and externally. We limit our exposure by making sure those internal and external vulnerabilities are addressed as quickly as humanly possible.” One of the *must* controls from the ISM states that all critical security patches must be applied within two days.

In presenting the security posture to business executives and the board, whether for purposes of addressing a particular issue or justifying a budget allocation, Knuth avoids technical details. “I approach it by outlining the business issue. It might be a matter of risk to brand reputation or the fact that we’re not meeting our obligations to the IMS.” Knuth recommends presenting the issue so that the executive board can understand the issue’s impact on the business. “Because it is a board-level decision,” he says, “I would explain the risk, the likelihood of the risk, and the risk rating based on our risk framework.” Knuth also says he would describe actual events to show in a tangible way the importance of addressing the issue. Knuth says it comes down to presenting security information in this way. “It is a high risk, and this is what I suggest we do about it. I need more money to do that. This is how long it will take, and this is what it will cost.”

“  
*I approach it by outlining the business issue. It might be a matter of risk to brand reputation or the fact that we’re not meeting our obligations to the IMS.*”



*You can select at most five metrics that are both qualitative and quantitative, and each [executive team] individual will pick up something he or she understands.*



  
LinkedIn

GENADY  
VISHNEVETSKY

CISO, Stewart Title Guarantee



## PIETER VAN DER MERWE

Chief Information Security Officer,  
Woolworth's Group

Pieter van der Merwe is the chief information security officer for the Woolworths Group, one of Australia's largest retailers. His responsibilities span the entire organization and include the establishment, development, implementation, and operationalization of a sustainable information security program. Pieter has more than 18 years of experience in information security and risk management around the world. His experience covers security strategy, architecture, design, network security, encryption, security governance and operations, vulnerability management, and information risk management.



Twitter | Website | LinkedIn



“How secure are we?” says Pieter van der Merwe, the chief information security officer for Woolworth's Group, “is a bit of a difficult question. There are the things you know and the things you don't know or you are not aware of. The way I typically answer that question is to provide the senior executives with a level of comfort of the coverage we have over the environment.”

Coverage, from van der Merwe's perspective, could be both technical and nontechnical. “We talk about the coverage and comfort level that we have as practitioners, in terms of infrastructure, applications, data, business processes and people. These are the five main things that we talk about, along with the level of understanding we have of the risks in each of these areas, and the risk mitigation plans in place to manage those risks.”

Van der Merwe says he addresses coverage using metrics related to administrative accounts, security assessments, critical data assets, and vulnerabilities on a high level, but he adds, “obviously, when they want to get into detail, we can delve down and see what that looks like.”

*“ We talk about the coverage and comfort level that we have as practitioners, in terms of infrastructure, applications, data, business processes and people. ”*

### KEY LESSONS

- 1 The technical comfort level of every executive is different. Some prefer more in-depth metrics, while others just want to know the basics, so it is essential to understand and communicate to the audience you're informing.
- 2 One way to reassure the CEO or the board is to demonstrate a clear understanding of the risks and ways to mitigate those risks without getting caught up in security-speak that holds no meaning to the business goals of the executive.



## DEMONSTRATE COMPETENCY AND COVERAGE, WITHOUT SECURITY-SPEAK

And van der Merwe uses two levels of identification to spot security weaknesses. “One is coverage; do we cover all of the assets (systems, applications etc.) The second one is whether we have confidence we have discovered all the technical security deficiencies within the specific system or application. We do this through vulnerability assessments, penetration testing, and project engagement reviews. Also, from an architecture and strategy perspective, I get our security architects involved in key decisions and discussions related to security risk identification and remediation from the inception phase of projects all the way through to production of the particular application or system. We are aiming for a culture of ‘Secure by design’”.

Security discussions with executives are driven largely by the topics the executives want to cover. “Some executives are more technically inclined, and want to know the technical details.” Even so, he adds, “Any conversation with your executives or board will be different than the conversation you will have with technology practitioners. Your board will typically be interested in whether management understands cyber risk and whether they have the appropriate measures in place to mitigate that risk. The risks most organizations typically focus on revolves around sensitive internal data and/or public disclosure of customer information” he says. “Whenever I have had a conversation with a board, they have not asked about technical details. Rather, they asked details about my plans and why I was confident that those plans will help us manage the risks we face. That’s where we, as security practitioners, get lost. I want to know how many vulnerabilities I have across my environment today, but boards typically don’t. They don’t have a reference point that helps them quantify the risk. We need to help them understand the actual risk to the business which will help the board quantify the level of investment required to manage the risk.”

“  
*Any conversation with your executives or board will be different than the conversation you will have with technology practitioners.*”



*If you put a robust security program in place, you can achieve compliance along the way, but it doesn't work in reverse.*



Twitter



Website



Blog

ED ADAMS

CEO, Security Innovation, Inc.





## ROSS SHERWIN DE CLARO

Senior Information Security Officer,  
Philippine Amusement and Gaming Corporation

Ross Sherwin de Claro is a highly regarded information security professional and Certified Ethical Hacker who is currently senior information security officer (ISO) in one of the most sought-after government agencies. As senior ISO, he advises the institution on how to protect from and prohibit attacks or exploitation of the information and network resources through effective information security, vulnerability, risk, and infrastructure management as well as enterprise architecture.



Twitter | Website | LinkedIn



When senior information security officer Ross Sherwin de Claro is asked to demonstrate the effectiveness of security systems for the Philippine Amusement and Gaming Corporation, de Claro happily points to the lack of system breaches for quite some time. He also cites the organization's strict compliance with government security requirements and guidelines, which are formidable. De Claro describes these via metrics from an administrative dashboard that is focused on the status of systems in the network that are considered most critical, and those that have been identified as most vulnerable based on the level of access that the operator has been given. In addition, de Claro's team regularly search for attempts being made to gain unauthorized access, at denial of service attempts and at the status of their Internet of Things (IoT) network.

While many of these data points report only the past and current readiness of the network, for de Claro, they are also the best glimpse into the future. This readiness is the result of close working relationships with software and systems vendors, which leads to good information sharing and quick responses when new threats appear.

*“When we implement new technology, it must integrate and talk to our existing technology fully, which allows for continuous monitoring and reporting.”*

## KEY LESSONS

- 1 Metrics that show past potentially hostile activities (denial of service attempts, log-in attempts, etc.) are good for showing that past actions have been successful, and they can also provide a glimpse into the future.
- 2 Keep management reports simple with a focus on how your group's performance compares with other, similar, operations, using comparable metrics.



The Philippine Amusement and Gaming Corporation comprises a network of 36 casinos regulated by the Philippine government. As a government agency, it is subject to strict national requirements as well as cross-country agreements such as those imposed by the Asia-Pacific Economic Cooperation (APEC) and the Association of Southeast Asian Nations (ASEAN). And though they do not yet need to meet this standard, de Claro has implemented most of the Payment Card Industry Data Security Standard (PCI DSS), partly in anticipation of future need. Additionally, because of their role as a gaming industry agency, de Claro's team follows those standards and metrics outlined for the casino industry by Gaming Laboratories International. These include intrusion detection and prevention, vulnerability scanning, antivirus and malware monitoring, encryption and other fairly typical security metrics.

In addition to showing management that his agency is ISO 27001 compliant and operating to all current standards, de Claro focuses on basic metrics that show the number of breach attempts that were unsuccessful. He can easily compare the security posture of his operations with other government agencies thanks to shared and standardized data. Comparisons can also be made to other gaming-industry metrics outside the Philippines.

Maintaining compliance with various government standards might seem to be a pretty straightforward task, but building confidence and remaining responsive to threats is a daily exercise for de Claro and his relatively small team of security professionals.

"Working with vendors is a two-way process," says de Claro. "We dictate which security technologies we want, and the provider gives us information about what's new in the industry, so we work together to meet our specific requirements."

At times, that collaboration requires bringing together two or more technologies from multiple vendors. De Claro uses a custom dashboard to review holistic data specific to his agency, and his team tracks complex levels of information, including layered securities, antivirus, perimeter gateways, network access control, and endpoint security.

“  
*Issues others have gone through have become a learning experience for us, and we always look for how our branches might benefit from these lessons. We look into international initiatives and attend foreign seminars.*”



De Claro's quarterly reports to management provide a glimpse into security details. These reports are also an important part of the yearly budgeting process, and can be critical when deciding where to deploy in-demand resources.

When de Claro is asked about the security health of his organization's IT infrastructure, he prefers to answer several distinct questions:

1. Does the agency comply with all relevant local and international guidelines and requirements?
2. Is there a channel of communications and is information sharing taking place with similar industry-specific organizations?
3. Does the team have the resources and data they need to keep abreast of developments on a daily basis, and adjust accordingly?

De Claro is constantly juggling resources as he balances the need for country-wide security in multiple locations with his small internal team. Indeed, de Claro often refers to mitigating low staffing issues with the placement of advanced technology.

"We have around 36 branches," says de Claro, "so the team must have extensive network visibility and needs to adapt dynamically to changes in those 36 branches, which can grow or shrink, sometimes rapidly. The technologies must be able to adapt to each specific situation. When we implement new technology, it must integrate and talk to our existing technology fully, which allows for continuous monitoring and reporting."

No industry operates in a vacuum, and de Claro isn't just content with metrics that simply reinforce how his agency is meeting Philippine government requirements.

"We regularly look at the implementation of casinos elsewhere, for instance, in Macau and Singapore, and even in Las Vegas," says de Claro. "Issues others have gone through have become a learning experience for us, and we always look for how our branches might benefit from these lessons. We look into international initiatives, we attend foreign seminars, and we attend gaming expos where vendors show us what they are developing for slot machines, table games, and other forms of wagering."



*It is important to raise issues using a risk-based language that allows the board to make risk-based decisions on cyber-security spending.*



 |  |  | [Twitter](#) | [Website](#) | [LinkedIn](#)

**SCOTT SINGER**  
CISO, PaR Systems, Inc.



Tenable transforms security technology for the business needs of tomorrow through comprehensive solutions that provide continuous visibility and critical context, enabling decisive actions to protect your organization. Tenable eliminates blind spots, prioritizes threats, and reduces exposure and loss. With more than one million users and more than 20,000 enterprise customers worldwide, organizations trust Tenable for proven security innovation. For more information, contact us at:

### **APAC Headquarters**

Tenable  
600 North Bridge Road  
#09-06 Parkview Square  
Singapore 188778  
+65-67186750  
[anz-sales@tenable.com](mailto:anz-sales@tenable.com)  
[sg-sales@tenable.com](mailto:sg-sales@tenable.com)  
[ph-sales@tenable.com](mailto:ph-sales@tenable.com)  
[th-sales@tenable.com](mailto:th-sales@tenable.com)  
[my-sales@tenable.com](mailto:my-sales@tenable.com)  
[id-sales@tenable.com](mailto:id-sales@tenable.com)  
[in-sales@tenable.com](mailto:in-sales@tenable.com)

### **Hong Kong**

Tenable  
Level 3, Three Pacific Place  
1 Queen's Rd East,  
Admiralty, Hong Kong  
[hk-sales@tenable.com](mailto:hk-sales@tenable.com)  
[tw-sales@tenable.com](mailto:tw-sales@tenable.com)

### **Shanghai**

Tenable  
Unit 37, 25th Floor,  
Central Plaza,  
381 Huai Hai Middle Road,  
Shanghai, China  
+86-21-6032 3549  
[cn-sales@tenable.com](mailto:cn-sales@tenable.com)

### **Tokyo**

Tenable  
Yusen building 1F,  
2-3-2 Marunouchi,  
Chiyoda-ku, Tokyo  
〒100-0005  
+81-3-5533-8643  
+81-3-5533-8644  
[jp-sales@tenable.com](mailto:jp-sales@tenable.com)

**Find more thought leadership information at: [CISO Resources](#)**

**Learn more about how other organizations are using Tenable solutions: [Case Studies](#)**