InfoSecurity PROFESSIONAL

How Do You Measure Up?
FINDING THE FORMULA FOR A SUCCESSFUL YEAR

Metrics that Matter
3 Steps to ‘Keying’ in on Performance
Playing ‘House’
Have your open enterprise and secure it too.

Opening your enterprise to new technologies that build your business no longer comes at the expense of Security.

Stop by our booth # 2709 at RSA Conference 2014 and visit us at www.ca.com/openenterprise to see how you can both enable and secure your business.

Copyright ©2013 CA. All rights reserved.
Great Expectations: Mastering Metrics to Gain Visibility
Metrics. Security professionals either love ‘em or hate ‘em. Regardless, everyone agrees: Metrics are a necessity.
BY CRYSTAL BEDELL

Security Metrics—Lost in Translation?
A security expert provides tips for coming to a meeting of the minds when talking security.
BY J.J. THOMPSON

A ‘House’ Full of Inspiration
Using a fictional medical diagnostician as a muse can help solve difficult cyber security mysteries.
BY KERRY A. ANDERSON
IN APRIL 2002, I wrote a piece for Information Security magazine about the IT security profession at a crossroads. Businesses back then recognized the need to [better] protect their digital assets and networks, but remained unclear about whom to hire to ensure that protection. Highly skilled hackers with questionable pasts were trying to go legit, while others on a more traditional career path strived to compete with them.

In that article, I mentioned an organization with growing influence and a prized credential, the CISSP, which I thought had the potential to both solidify and shape a then-nebulous industry. That organization, of course, was (ISC)².

Much has happened in the 12 years since I penned that piece, with both the organization and its impact. (ISC)² has evolved into a mosaic of global communities melded by a desire to thwart cyber threats and help their enterprises grow.

The latter goal is a relatively new one for those more comfortable working in silos. That’s why we focus this issue on setting and achieving goals. Contributor Crystal Bedell speaks with experts on why security metrics are so important. And J.J. Thompson, a data security strategist and (ISC)² Indianapolis Chapter president, takes it to the tactical level to help ensure success all around.

Finally, another (ISC)² member, Kerry Ann Anderson, shows how a favorite fictional television character helped her get to the root of security issues. The show currently runs in syndication all over the world, and may spark some creative problem-solving for you, too.

The best part is these same principles apply to our personal lives, not just professional lives. Here’s to a successful year for one and all!

Anne Saita, editor-in-chief, lives and works in Southern California.

For information about advertising in this publication, please contact Tim Garon at tgaron@isc2.org.
Save time and money at Capella University

The knowledge you gained for your IT certifications—including CISSP®, CISA®, CISM®, and more—can help you earn college credit toward a Capella bachelor’s or master's IT program, saving you time and money on your degree.

Online degrees in key IT fields

Further your career—explore Capella bachelor’s, master’s, and doctoral degrees in:

- Information Assurance and Security
- Project Management
- Network Technology
- And more

Many Capella IT programs have earned national recognitions and designations from several organizations, including:

- Project Management Institute (PMI®) Global Accreditation Center for Project Management (PMI-GAC)
- National Security Agency (NSA) Designation for Information Assurance Education (CAEIAE)
- U.S. Department of Homeland Security (DHS)

Put your IT certifications to work: capella.edu/ISC2 or 1.866.646.8128

Washington residents may receive credit through Capella’s prior learning assessment only in the bachelor’s and MBA programs. Capella’s BS in IT program is accredited by the Computing Accreditation Commission of ABET, http://www.abet.org. The following program specializations are accredited by the Project Management Institute (PMI®) Global Accreditation Center for Project Management (PMI-GAC): BS in Information Technology – Project Management, BS in Business – Project Management, MS in Information Technology – Project Management, MBA – Project Management. Capella University has been designated as a NSA/DHS national Center of Excellence for Information Assurance Education (CAEIAE) for the academic years 2012–2017.

© 2014 Capella University. 14-7487
SILVER LININGS
OUR 25TH ANNIVERSARY IS FOCUSED ON THE FUTURE RATHER THAN REFLECTING ON THE PAST

WENTY-FIVE YEARS ago a group of volunteers organized to elevate the IT profession by offering a body of knowledge [now known as the (ISC)² CBK®] and a new credential to bolster the work of those with a passion, not just a passing interest, in information security.

That year, 500 people applied to be a CISSP, a sure sign those volunteers were on to something. Today, (ISC)² has some 95,000 members in 135 countries seeking similar professional growth.

Today, (ISC)² is far more than a consortium of credential programs; it’s a true community, demonstrating strength in membership.

Our members gather over coffee and over conferences to provide expertise, discuss the latest cyber threats, and determine how to thwart them. Through (ISC)², members are involved in standards development and skills mapping for the industry. They share ideas and ideals within (ISC)² Chapters and in ways hard to imagine in 1989, when most of the consumer world remained unaware of the Internet, email, and social networks that are now the norm.

We’re proud of all we’ve accomplished since our early days. But like a typical 25-year-old, we’re more focused on a long life ahead and how best to make a lasting impact.

As such, we will continue to broaden our educational programs and offer specialized certifications to meet a maturing profession and more demanding workforce. As the challenges to global information security become more sophisticated, (ISC)² is dedicated to refreshing our certification and training programs to meet the needs of an ever-evolving threat landscape. Forward thinking to anticipate and protect against these threats with the highest level of integrity, diligence, and expertise is paramount to the success of our members and their organizations. Last year, we introduced the Certified Cyber Forensics Professional (CCFP℠) and HealthCare Information Security and Privacy Practitioner (HCISPP℠). This year, we are launching a new credential for those specializing in cloud security.

Through expanded services, webinars, forums, chapters, and strategic partnerships, we are providing our members with increased CPE and training opportunities in addition to expanded tools to stay current in their respective profession. We constantly strive to keep all credential programs relevant to the industry, while also helping to ensure that an (ISC)² membership always carries clout. We also want to continue providing employers with confidence that an (ISC)² member has the skills, knowledge, and professional network needed to protect their companies and comply with all regulations.

By being the leading voice in security, we assist emerging markets and economies, with tailored education and training.

We’ve also taken our mission to inspire a safe and secure cyber world to newer generations of end-users through the (ISC)² Foundation’s Safe and Secure Online Program for children.

Whatever future technological or business issues our members may encounter in their careers, rest assured that (ISC)² will help them rise to the challenge.

Elise Yacobellis is the (ISC)² Director of Global Development and Executive Publisher of InfoSecurity Professional.
WELCOME TO THE NEW STANDARD IN CYBER FORENSICS

No cyber forensics credential provides a comprehensive validation of your knowledge and skills as a digital forensics expert.

UNTIL NOW

CCFP is the definitive credential that demonstrates your ability to:

- Deliver accurate, complete, and reliable digital evidence
- Assure digital evidence is admissible in a court of law
- Tackle a broad array of challenges from intrusion analysis to mobile forensics and more

CCFP Webcast Series
Subscribe to the CCFP domain previews to watch 10-15 minute webcasts on each of the domains, the value of the credential and what to know for the exam.

Watch Now
A ROUNDUP OF WHAT’S HAPPENING IN (ISC)² COMMUNITIES

NEW FORMAT, HOTSPOT QUESTIONS ON CISSP EXAM

This year (ISC)² is introducing a new feature and a new topic on the CISSP certification exam. The first is a new “drag & drop” feature for questions that is designed to:

• Measure knowledge at higher cognitive levels;
• Measure a broader range of skills;
• Provide more realistic simulation of practice in the field;
• Provide opportunities for broader content coverage than may be possible with multiple choice questions.

Additionally, there will be new questions on securing hotspots on this year’s exam.

What won’t change is the amount of time allotted to complete the test, nor how questions are scored.

MORE DAYS—AND WAYS— TO PLAY IT SAFE

The Safe and Secure Online Program continues to empower and educate children, parents, teachers, and, soon, seniors on the importance of cyber safety, cybersecurity, and the ever-growing issue of cyber ethics. Our volunteers geared up in recognition of International Data Privacy Day, which is celebrated each year on January 28th and is an international day of awareness to empower people to protect their privacy and control their digital.

CONTINUED ON PAGE 10

SPOTLIGHT ON...

(ISC)² ITALY CHAPTER IS NEW OFFICIAL TRAINING PROVIDER

THE (ISC)² ITALY Chapter was established in July of 2012 by certified professionals who work to protect IT systems and data from disruption and cyberattack within companies from all sectors, including financial services, manufacturing, technology, and healthcare. The Chapter covers most major cities in Italy and is open to anyone who would benefit from their programs.

The Italy Chapter has grown to over 180 members, with a significant membership in both Rome and Milan. Efforts are underway to develop active groups in the country’s other major cities. The Chapter has a no-fee membership, which is an important element of their strategy to continue rapid development throughout the country. “There was no chapter in 2011 and today we are among the most popular and respected security associations in Italy. We are all proud of this,” says Massimiliano Macri, board member, (ISC)² Italy Chapter. In Italy, there are less than 250 (ISC)² members; however, approximately 30% of Italian (ISC)² members belong to the Chapter.

The Italy Chapter offers opportunities for individuals to network and

CONTINUED ON PAGE 10

ITALY

18 months since its July 2012 charter

180 approximate number of chapter members since its inception

4,000 number of schoolchildren, parents and teachers receiving security awareness sessions by chapter

Photograph ©Claudio Divizia–iStock–Thinkstock
(ISC)^2 and MIS Training Institute invite you to engage in cutting-edge learning and to network with more than 1,300 security professionals from around the world!

(ISC)^2 Featured Events at InfoSec World 2014 include:

- **(ISC)^2 CISSP® CBK® Training Preview**
  Tuesday, April 8, 1:55 PM - 5:00 PM
  [Click here to register!](#)

- **(ISC)^2 2-Day Workshop**
  Saturday, April 5 & Sunday, April 6, 9:00 AM - 5:00 PM
  W2 “Fundamentals of Business Acumen and the Security Professional”

- **(ISC)^2 Member Reception**
  Tuesday, April 8, 6:15 PM - 7:45 PM
  ([ISC] Members only, click here to register!)

With 7 tracks, 11 in-depth workshops and 3 co-located summits, InfoSec World promises to deliver practical, technical sessions that give you the tools to strengthen your security without restricting your business.

TO REGISTER     PHONE 508.879.7999     ONLINE [www.misti.com/infosecworld](http://www.misti.com/infosecworld)
increase their visibility through events and social networks. Specific activities include: hosting the (ISC)² Secure Leadership Series in Rome in July; the delivery of monthly learning webinars; contribution to the Italy Security Landscape book; participating in major security and ICT conferences across the country; and the delivery of security awareness sessions in schools reaching more than 4,000 children, parents, and teachers.

In December 2013, the (ISC)² Italy Chapter hosted its first Official (ISC)² CISSP® Training Seminar in Rome. CLUSIT, the Italian association for IT security, first introduced the CISSP certification to Italy, and now supports the (ISC)² Chapter with certification training. Additional training will be hosted in Milan in 2014.

“Our Chapter’s mission is to make a difference in ICT and physical security by consolidating the role of the security professional along the lines of the (ISC)² Common Body of Knowledge (CBK®),” states Macri. “We work hard to evangelize for the ICT security profession and professional certifications, while providing guidance for those willing to achieve a professional certification. Delivering the training was a logical next step.” He reports that the chapter has received a number of inquiries about the program.

The Italy Chapter chose to become an (ISC)² Official Training Provider to support its members, 50% of whom are non-certified, and to improve general security practices in Italy. CLUSIT will continue to promote the training program to its membership and 5,000 newsletter subscribers.

(ISC)² ITALY CHAPTER CONTACT INFORMATION

Name: Claudio Sasso  Email: info@isc2chapter-italy.it
Website: http://www.isc2chapter-italy.it/
LinkedIn: http://www.linkedin.com/company/-isc-2-italy-chapter

APPLICATIONS DUE APRIL 1 FOR (ISC)² FOUNDATION GLOBAL SCHOLARSHIPS

The math is simple: A high demand for skilled cyber security experts and low supply of qualified candidates equal a world of opportunity. The (ISC)² Foundation aims to bridge this gap by providing future information professionals with scholarships to prepare them for a rewarding career in this important field. The 2014 (ISC)² Foundation Global Information Security Scholarship Program is accepting applications through April 1. The (ISC)² Foundation will be awarding multiple, qualified applicants across the globe with Women’s, Graduate, and Undergraduate Scholarships, in addition to Faculty Exam Voucher awards for those educating our future security professionals. Please visit www.isc2cares.org for more information.

CPEs

When submitting CPEs for (ISC)²’s InfoSecurity Professional magazine, please choose the CPE Type: “(ISC)²’s InfoSecurity Professional Magazine Quiz (Group A Only),” which will automatically assign 2 Group A CPEs.


Photograph ©PG Gutenberg UK Ltd–iStock–Thinkstock


**CISSP, EDUCATION PROGRAM ARE FINALISTS FOR 2014 SC AWARDS**

_**THE CISSP, CONSIDERED**_ the gold standard of certifications for information security competence, is again vying for “gold” at the upcoming 2014 _SC Magazine_ Awards. The certification is a finalist in the “Best Professional Certification Program,” while, for the second year in a row, the (ISC)² Education Program is up for “Best Professional Training Program.”

Though nominated in separate categories, the two programs are connected to a greater goal of providing information security professionals with the skill sets and knowledge necessary to advance in their careers and keep their employers safer from future cyber threats.

Last year, (ISC)² increased member accessibility to study tools and brought its educational products more in line with adult learning strategy and sound instructional design theory, providing candidates with a better all-around learning experience while strengthening their knowledge base. Additionally, the organization introduced new educational formats including seminars that provide students a hands-on experience to utilize the knowledge they gain from the classroom environment. The multitude of learning platforms offered by (ISC)² provide students the convenience and accessibility to grow and advance in their careers.

An expert panel of judges considered factors such as applicable research, analyst reports, and product reviews in narrowing the field from a host of nominations. SC Award winners will be announced at a gala on Feb. 25 in San Francisco.

“Technology lost many battles for the defenders in 2013, but those losses taught us a valuable lesson—that the capabilities of technology are extremely limited unless they are supported by an army of security professionals that is strong in numbers and honed in its skills. Armed with this lesson, I believe that the tide in the cybersecurity war could turn in 2014—and the defenders with the strongest human skills will have the advantage.”

—W. HORD TIPTON, CISSP, (ISC)² Executive Director in a Dec. 20, 2013 blog post
2014 (ISC)^2 BOARD OF DIRECTORS

BELGIAN WIM REMES NAMED CHAIR

Wim Remes, CISSP, in late January was named the new chair of the (ISC)^2 Board of Directors.

Remes, who hails from Belgium, will be joined in the leadership circle by Vice Chair Prof. Corey Schou, PhD, CSSLP, and Fellow of (ISC)^2 (U.S.A.); Secretary Dave Lewis, CISSP (Canada); and Treasurer Greg Thompson, CISSP (Canada).

A former manager of information security for Ernst & Young and security consultant for Bull, Remes is now a managing consultant with OIActive and has 15 years of security leadership experiences. He’s an international speaker who has worked on numerous information security initiatives such as co-developing the Penetration Testing Execution Standard (PTES), InfoSecMentors, the Eurotrash Security Podcast and organizing the BruCON security conference.

This 2014 (ISC)^2 board also includes:
- Diana-Lynn Contesti, CISSP-ISSAP, ISSMP, CSSLP, SSCP (Canada)
- Dan Houser, CISSP-ISSAP-ISSMP, CSSLP, SSCP, CISSP (U.S.A.)
- Greg Mazzone, CISSP (Australia)*
- Jennifer Minella, CISSP (U.S.A.)*
- Richard Nealon, CISSP, SSCP, CISA, CISM (Ireland)*
- Prof. Jill Slay, CISSP (Australia)
- Prof. Howard Schmidt, CISSP, CSSLP (U.S.A.)*
- Freddy Tan, CISSP (Singapore)*
- Prof. Hiroshi Yasuda, Dr. E, CISSP (Japan)

*Named to board in December 2013
AS I REFLECT on 2013, my thoughts keep drifting to one essential question I am sure many of us are thinking: How successful was I as a security professional this past year? Naturally, this causes us to evaluate how we actually define success.

Did we have to disclose any breaches? Were my projects completed on time and on budget? Speaking of budgets, did mine grow or shrink for the next year? Did I meet my compliance obligations?

Each of these are valid questions that I have heard our peers asking, often in hushed tones over a post-work beer, but I think we are perhaps missing the bigger picture. We are too narrowly defining our success, or lack thereof.

As the custodians of our enterprise security programs, either as teams or as individuals, we need to take a fresh look at how we not only define our success, but also in how we measure it—and how frequently. So far, in my discussions across our community, I have heard that there is a gap between how we define our own success and how our various stakeholders view our programs.

As we embark on a new year, I encourage each of you take a moment to reflect on your own experiences around security metrics and reach out to me with your thoughts. I’ll be driving for more clarity on this topic through not only the live, in-person events, but also on our webinars and e-symposia.

Until next time, please keep in touch, and I look forward to continuing the conversation.
Great Expectations: Mastering Metrics to Gain Visibility

security is like any other management discipline. Risk is a fundamental of whatever management science you want to apply. It comes down to: ‘Am I, as a custodian of the limited resources, making a judicious decision in my application of those resources that allows the organization to succeed in its mission?’ says Brandon Dunlap, managing director of research for Brightfly Consulting.

There are two primary reasons why security professionals track metrics.

Ben Mayrides, president and principal for Acureti, explains further: “First and foremost, to make sure that your information security program is meeting organizational objectives, whether related to security objectives or a larger objective. Security metrics should reflect and achieve objectives in a broader risk management set of objectives for the organization.”
Secondly, metric tracking can guide security investment decisions. “The security professional has to guard against literally an infinite number of attacks, but an attacker only has to find one method to achieve their goal,” declares Caroline Wong, security initiative director for Cigital and author of Security Metrics, A Beginner’s Guide. “You’re always going to have limited resources. How do you invest those resources to get the most bang for your buck? That is the answer I think security metrics can answer.”

Mayrides agrees: “So often, information security, IT security, and other elements of security are considered a cost center for the organization. You want to make sure that the investments you’re making as an organization and in information security provide some sort of return on investment. Having a decent set of security metrics helps to tell that story to top management because they are typically concerned about the top line as well as the bottom line, and tracking the cost of internal investments: And security is typically one of those things.”

**WHY COLLECT SECURITY METRICS**

There are several benefits to collecting security metrics. “The first benefit is visibility; understanding what’s going on. What is my security state today?” Wong explains.

Security metrics, she adds, can also help establish a common lexicon between the security team and everyone else. “The effective use [of metrics] can lead to a common language so that security people can talk to non-security people about security things and help them make decisions about things that aren’t their primary area of expertise.”

Finally, security metrics can help drive change, and this is a reflection of the first benefit—understanding what’s going on today—and the second benefit, which is having a common language for stakeholders, Wong explains. “Oftentimes, in order to make real change happen, it can’t happen just by security professionals. It requires buy-in from stakeholder and sponsor groups to attain resources.”

Mayrides echoes this sentiment: “If you have metrics and they’re mapped to risk management objectives, and they are mapped to organizational objectives, and you’ve had that previous discussion with management, then I think you can expect movement or change,” he said.

For example, Mayrides explains, if an organization relies on third parties for a portion of its data security strategy and it conducts a risk assessment of those third-party vendors or service providers and identifies a series of risks, and those findings can be mapped to top management’s concerns and risks you’ve highlighted previously, then you should be able to influence management’s decision-making. Management may decide to strengthen the contractual language with those providers or conduct annual risk assessments of the providers.

“It’s not just the metrics that are important,” Mayrides adds. “I think it’s important that the metrics themselves are considered as one key piece of that conversation with management.”

**WHAT TO MEASURE**

Along these lines, there are two primary types of metrics that security professionals collect. Evan Wheeler, director of IT risk management for a global financial services organization and author of Security Risk Management: Building an Information Security Risk Manage-
ment Program from the Ground Up, describes these as performance and activity metrics. Performance metrics reflect how well the risk program is functioning while activity metrics demonstrate the organization’s efforts.

“Both are needed, but as you get more mature, you focus less on the activity metrics and more on the performance metrics,” Wheeler explains. “When you first begin a program, to say how well you’re doing, you have nothing to compare yourself to. Activity is all you can report on, but as you get more mature, you have more baselines to report on.”

Experts warn that simply measuring particular threats that are coming at the organization is of little or no use. “The metric you track isn’t how many criticals you have at any time,” offers Dunlap. “The metric you track is how long it takes to close a given vulnerability, because that’s the window of opportunity for my attacker. Once I become aware of it, I know everyone is aware of it. How quickly can I resolve those faults in my system? I have limited resources; where do I apply them?”

Wheeler also suggests measuring key risk indicators as related to the organization’s inherent risks. “For every control you consider implementing, you should have some risk indicator that tells you whether that control is successful or not,” he says. “You have to fundamentally think about what that control is trying to achieve.”

For example, if you have an email blocking solution in place that is blocking credit card numbers, what would you use as a gauge to determine whether the control is doing its job? And is it good if the number of blocked credit card numbers increases because the control is doing its job or bad because people keep sending them out? This should be determined in advance, but either way, when the threshold is exceeded, it should be an indication that something needs attention.

“It’s not the whole story, but the catalyst to go do research,” Wheeler adds. “You can’t spend all of your time managing all of the controls. You need metrics to tell you when it’s time to go look at something.”

BEST PRACTICES FOR REPORTING METRICS TO MANAGEMENT

Experts have plenty of advice for reporting metrics back to management.

“I jokingly have two tests,” Cigital’s Wong says. “One is the so-what test and the other is the who-cares test. If you are a security professional and someone says so what or who cares, then there’s probably a better way to present that information.”

Your audience should dictate how you present the information, according to Wheeler: “One of the most important points is [to] know your audience. The metrics you review with the security and risk team are different than what you’ll review with the risk committee, and those are different from the metrics you’ll review with your board. They’ll all be based on the same things, but focused on different areas.”

Regardless of your audience, Wong says keep the message simple. “If you’re including a lot of data in your communications, make sure the data makes sense to the person you’re including it to; because if it doesn’t, it’s a waste of your time, their time, and a distraction.”

Mayrides agrees: “You typically want to make sure information presented to management is timely and accurate, and presented in a context for management to make a decision.” If you don’t, he warns, you could be faced with an executive team that not only doesn’t understand the issues, but disregards your efforts on the company’s behalf.

CRYSTAL BEDELL is a freelance writer specializing in information security.
Europe’s biggest information security event!

29 April to 01 May 2014 | Earl’s Court, London UK

Network, engage and do business with +15,000 information security professionals at the 19th Infosecurity Europe!

Why should you attend?

- Meet with 325+ industry-leading vendors and suppliers.
- 100+ hours of free high-quality education to develop your career and skills.
- Earn CPD and CPE credits from attending the free education programme sessions.
- Exclusive access to industry experts, keynote speakers and thought leaders.
- Network with peers, share knowledge, collaborate and build relationships.
- Gain access to new and innovative security solutions.

Register free* now at:
www.infosec.co.uk

Engage with Infosecurity Europe on Twitter: @infosecurity #infosec14

* Online registration closes Monday, 28th April 2014 at 12:00 GMT. Onsite registrations will be charged at £35.
IT’S NOT GOING WELL. Your boss scans the metrics you presented and says for the umpteenth time, “This is close, but something is just not quite right.” Your pulse pounds in your head. You wisely bite your tongue. You’d like to say: “We’ve been going in circles on this because you simply don’t understand how security works! Tell me what you want and I’ll figure out a way to map into it. …OK, fine. I’ll give you what you asked for, but I guarantee it isn’t going to get us where we need to be.”

Instead, you simply reply, “I’ll take another stab at it.”

As you head out of the conference room, you can’t help but think that there has to be a better way to bridge this gap. And you’re right. There is.
Misalignment in metrics communication is not the fault of the audience; it is a problem with the person holding the microphone. To solve this issue, you have to align your messaging with a central theme that can be modified as needed to effectively manage emotional reactions to news of emerging threats and media hype, while maintaining true north on your strategic compass.

In other words, you need to bridge the gap between what managers think they need to hear and what they actually need to hear—and in a language everyone understands.

**Misalignment in metrics communication is not the fault of the audience; it is a problem with the person holding the microphone.**

Not only does security need to be scalable and cost effective, but thanks to the marketing messaging behind such hot topics as virtualization and cloud capabilities, it has to meet board members’ expectations shaped by news media alerts on the latest advanced persistent threats. Those often unrealistic expectations can increase or decrease security resources at a moment’s notice.

In the news media, there’s the old saying: “If it bleeds, it leads.” In cybercrime, it’s more like: “If it shakes your board and executive team to the core and makes them think they are about to live through an episode of 24 meets The Blacklist,” then you’ll probably see an email about it in the morning and your entire security strategy may change on the spot.

Because of external factors outside of your control, you need to be in a position to continually shape the message while maintaining strategic direction and plans. Members of Security Operations Centers (SOCs) need to demonstrate that they understand the board’s expectations in IT security and remain nimble enough to move around at a moment’s notice to address emerging threats and decrease investments in lower priority activities.

Based on our client base and conversations with industry leaders, security teams struggle to provide management with the transparency and metrics needed to give them the “dial” they desire for three reasons:

1. Improperly defined security service catalog
2. Failure to align with IT operations models
3. Absence of outcome-based metrics

Each reason above is, in itself, a critical path item for successfully managing and running a SOC, yet each failure above can be broken into its component parts to determine if this affects your team or to validate that your program is on the right path. Below are the keys to getting your security team back on track with the next generation of executive expectations around security metrics.

**1 Define the security service catalog**

When executives are asked what security services their team provides, what do they say? Is there a well-defined services catalog that breaks down what the internal service offering is, who performs it, how it’s performed, and what the inputs and outputs are? What about SLAs?

Many companies have a hard time elaborating on what they do and how they do it in a measurable way. Key indicators of success include a formally defined security service catalog (think the Information Technology Infrastructure Library, or ITIL) that is documented and well communicated. This service catalog should also be supported directly, not just on paper or in work sessions, by processes and capabilities that deliver and monitor delivery success.

**2 Align with IT operations models**

One of the biggest challenges that companies went through in the 2000s was how to measure what IT is and what it accomplishes for the business.

IT leadership spent a lot of time on this and ended up in two buckets: (1) IT models that are formally...
defined and measurable; and, (2) those that were “executive friendly” looked good on a slide, but did not link strategy to capabilities to metrics.

For our purposes, we’re focusing on the former case, as many of these organizations headed towards ITIL. In short, the IT operations measurement model for tracking effectiveness broke down into the components of Availability Management (time to detect, time to record, time to diagnose, time to repair, time to recover). This fundamentally shaped the way that modern service desk solutions were designed and the associated flows that are reported for each and every IT availability issue in mature IT organizations.

In these companies, did the security team play by the same rules, or were they too difficult? Did security push back by saying it didn’t work that way for security incidents? The best aligned organizations figured out how it was similar and fit into the model—specifically when it came to understanding that a core security infrastructure (FW, IDS, IPS, SIEM) had to work effectively to allow “time to detect” to be measurable.

Then, time to record is pertinent as those tools need to be configured to place only the most likely incidents into the ticketing system for the security analysts to review. Security analysts also need to conduct their diagnosis and document the next steps that are needed in a simple, concise, and easily actionable manner for their IT infrastructure or business counterparts to take action on the incident.

This is also where security goes awry. Often, incident tickets become the holding place for the associated change requests and problem management tickets as well. This is how security claims that “our incidents don’t fit into the ITIL model.”

Not so.

Security needs to focus on learning the differences between incidents, problems, and change requests so they can properly measure and monitor performance.

3 Focus on outcome-based metrics

All metrics are not created equal. The best SOCs utilize metrics that drive an adjustment, a change of behavior or result in security resource adjustments.

It’s no longer sufficient to provide the total count of identified vulnerabilities; volume doesn’t map to an outcome or adjustment. Instead, report on the count of vulnerabilities that are net new (newly discovered since the last scan), exempted (known but risk accepted) or carry forward (previously identified, but still unresolved).

Each of these cases is due to a different root cause, and therefore requires a different path to resolution. The count of vulnerabilities simply doesn’t provide the requisite information for a change of behavior that results in an improved outcome.

Consider:

• How many mentions were there of your company on public hacker paste sites?
• How quickly did you detect and determine if they were incidents or just events?
• For incident management, are you able to track the events per second or GB/day of your logging usage?
• How about the number of protected nodes?
• What about the number of third-party identified incidents that were not caught by your core security team?

Each of these metrics should lead to a discussion about what can tactically be done to alter the outcome of the metric (hopefully for the better) by the next review period. Make sure to emphasize how metrics can be tracked, trends identified, and actionable results taken to make measurable improvement in the metric in short order.

The metrics problem is not new and it is not going to be eliminated by a silver bullet solution.

There needs to be convergence of a board focus on security, an IT team that can translate its challenges into business-aligned action items, and a way to generate the type of reports using metrics identified as the best course of action to meet those challenges.

If you embrace the challenge and adopt simple, strong messaging that you continually reshape ahead of executive concerns, you will be in a position to bring forth positive change through security metrics that matter.

J.J. THOMPSON, CISSP, is CEO of Rook Consulting and president of the (ISC)² Indianapolis Chapter.
HCISPPs are the protectors of personal health information.

Get the foundational global certification that validates your core knowledge and experience as a healthcare security and privacy practitioner.

DOWNLOAD THE HCISPP EXAM OUTLINE!

cert.isc2.org/hcispp-exam-outline
A ‘HOUSE’ FULL OF INSPIRATION

Using a fictional medical diagnostician as a muse can help solve difficult cyber security mysteries

BY KERRY A. ANDERSON

Following a number of plane crashes due to pilot error, the airline industry turned to NASA safety methodologies to develop pre-flight checklists to improve safety records. The same principle of borrowing best practices from another discipline works for information security practitioners, too.

Even those practices written for fictional television.

I admit some of my inspiration comes from the Emmy Award-winning network drama House, which ran for eight seasons and featured a brilliant but controversial medical diagnostician named Dr. Gregory House. He solved medical mysteries with the assistance of his multidisciplinary team, using both traditional and unconventional techniques to arrive at the root cause of a patient’s unusual illness.
In making a medical diagnosis, a doctor is like a detective, taking in clues in the form of symptoms, using knowledge and diagnostic tools to discover who or, more accurately, what dunnit. Even after a likely diagnosis, health practitioners typically continue to reassess their findings and adjust course during treatment.

A similar situation occurs in information security when searching for the root cause of a security issue, such as anomalous log entries.

• When did the “symptom(s)” begin and/or first become evident?
• Are you aware of other events, such as patching or an application install, occurring around the same time that the “symptom(s)” started?
• Has other similar or unusual activity occurred prior this event?
• How is this situation different from expected conditions?
• Are there any new or unexpected files/data on the system?
• Are files/data missing?

With a nod to various episodes from House, here are some recommendations for employing a diagnostic methodology to determine the source of security issues.

**Think Horses, Not Zebras**

One common piece of wisdom among medical practitioners when diagnosing patients is to “Think horses, not zebras.” Horses are more common than zebras. It is not that zebras do not exist; they are just the exception rather than the rule. Always look for the most common scenarios and simplest explanations first when confronting an information security issue.

For instance, one company discovered that a rapid number of CAPTCHA queries required for Google searches triggered a network alert. The security team initially believed the culprit was exotic malware on a network device, but the actual explanation turned out to be much simpler. A student intern (and, apparently, very proficient typist) doing some phone number lookups triggered an alert by exceeding the queries in quick succession coming from one IP address.

**What Is “Normal”**

It is important to know what qualifies as “normal” for an organization, especially when dealing with diagnostic tools such as logs. Otherwise, your information security team is less likely to understand uncommon activity.

**It is important to know what qualifies as “normal” for an organization, especially when dealing with diagnostic tools such as logs.**

For instance, doctors often look at a patient’s medical history or tests to determine what is normal for that individual before following up on other possible reasons for an ailment, such as a quirky heart rhythm or unusual blood chemistry reading. In security, this means getting to understand logs intimately before a problem occurs so you can create specific exception reporting entries.

**Whiteboard It**

Humans are visual creatures. Sometimes getting the data up on a whiteboard in front of the team or even yourself can stimulate theories of potential causes or new avenues of exploration. The visual presentation of competing theories can encourage some robust brainstorming and produce side-by-
side comparisons of different hypotheses that later are supported or eliminated.

RECOMMENDATION: Get the data up on a whiteboard (or flip chart) in front of the team with the following objectives:

- Eliminate alternative theories that do not fit the symptoms of the problem.
- Rank potential root causes by the degree of “fit” with the majority of symptoms.
- Determine additional testing methods to substantiate or eliminate remaining potential root causes.

Look to the Past

Surely, you have heard the adage that history “repeats itself.” Sometimes things occur almost identically. Other times, an old incident reoccurs with a slight variation but same root cause.

“If you watch closely, history does nothing but repeat itself. What we call chaos is just patterns we haven’t recognized.”

—Novelist CHUCK PALAHNIUK, Survivor

Just as health care providers attempt to get an accurate medical history, so too should information security professionals look to the past for what might play a significant role in present activities, such as older applications running on the server or applications created using a common development library. Also, investigate to see how the same issue was resolved (or not resolved) in the past.

RECOMMENDATION: Look for occurrences of similar incidents in the past and their potential root causes and resolution. If something fixed a problem before, it could likely work again. If it is a continuing problem, such as weak passwords on servers, it might be time to address the issue at a macro level to prevent future recurrences.

Look for Differences

Many television seasons before House, the children’s program Sesame Street presented a regular segment where characters looked for similarities in numerous objects to determine which was different.

Translated to information security, if two servers use a standard image and later only one host displays specific security vulnerabilities, a possible tactic might involve looking at the change control history or applications hosted on that server. By comparing configurations, software and the change histories of devices or applications, often the disparities may yield the source of the issue and potential clues about how to resolve it.

RECOMMENDATION: Consider differences as well as similarities when trying to diagnose a security issue. Minor differences between two devices can create an exploitable vulnerability. When faced with two similar devices with only one exhibiting a security issue, go back to your preschool days and ask yourself, “Which of these things is not like the others?”

Trial and Error

Sometimes you need a few failed experiments to come up with the real cause.

If trial and error testing is passive, there is usually limited risk. However, if testing is active and has the potential to create negative impact—such as updating live data, degrading performance, corrupting files or shutting down the system—any trials need to be approached with caution and should include a fully-considered recovery plan.

Remember, too, that trial-and-error testing initially can make a situation worse before you arrive at the best solution.

RECOMMENDATION: Sometimes, there is no option except trial and error to determine the root cause of a cybersecurity issue. However, trial and error can get ugly and preparation is vital to recovery if things go south. Trial and error is often the route Dr. House has his staff take just prior to his usual epiphany near the end of the show. In House’s scenario (it is a television program, after all) failure (i.e., death of the patient) is rare. With trial and error, you can either look brilliant or have to run for cover.
Either way, it usually gives you the answer or at least more information about the cause of the problem.

‘Perfect Storms’ are Rare...But Do Exist

Some cybersecurity issues can result from a “perfect storm,” where rare conditions converge. When the right combination occurs, the consequences can range from minor to catastrophic.

A multi-factorial root cause should not be the first avenue of investigation for a cybersecurity issue; it should be pursued only after excluding simpler explanations for a problem.

RECOMMENDATION: If, after excluding all simpler explanations for an issue, no single root cause can be determined, then it is appropriate to consider that multiple factors contributed to the creation of the security problem.

Use Gut Instinct, When Appropriate

Sometimes, you need to rely on your intuition—especially if all else fails.

Going with your gut should not be a first response; instead, act on intuition only after scrutinizing all the factors related to the situation.

RECOMMENDATION: Experience may help one intuitively recognize symptoms or new variations of former problems. However, relying on gut instinct alone can backfire—if not tempered with prudence. Sometimes, what we refer to as “gut instinct” may be the first idea that enters our minds. Balance that intuition with an appropriate level of cognitive reasoning.

Using a diagnostic approach to determine the root cause of a security issue can provide a framework for the investigative process. It can thwart the premature rush to the wrong conclusion by offering a structure to consider the possible alternative theories regarding what is creating the security issue. The diagnostic approach works for both a sole practitioner and a team.

A primary advantage to this methodology is that it favors looking at the simplest explanation first rather than a more complex hypothesis.

By applying Occam’s Razor—“the simplest of competing theories [is] be preferred to the more complex,” according to Merriam Webster—we are guided to developing a potential diagnosis of the cybersecurity issue and its cause(s) by first removing any inconsistencies, ambiguities, and redundancies that might cloud the issues.

However, there’s always one last possibility. As Dr. Gregory House once wryly said, “Occam’s Razor: The simplest explanation is almost always somebody screwed up.”

KERRY A. ANDERSON, CISSP-ISSAP, ISSMP, CSSLP, CISA, CISM, CRISC, CGEIT, CFE, CCSK, MBA, MSCIS, MSIA, is an information security and records management consultant with more than 15 years of experience in information security and IT across a variety of industries. She is currently an adjunct professor for Clark University Cyber Security Graduate Program and under contract to write a book on information security management.

“In 2008, House was distributed in a total of 66 countries. With an audience of over 81.8 million worldwide, it was the most watched television show on the globe…” —Wikipedia
WE’VE KNOWN FOR a while that the demand for skilled information security professionals outstrips the supply. Despite strides made in recent years to fill that gap, the expanse remains.

A new white paper, “Critical Times Demand Critical Skills,” shines a light on the job in greatest demand (regardless of the industry, region or even nation): the security analyst.

That’s the finding based on 12,000+ respondents worldwide who were part of the 2013 (ISC)² Global Information Security Workforce Study conducted by Frost & Sullivan, in partnership with Booz Allen Hamilton.

Security analysts are people with broad responsibilities requiring a wide range of skills. They are charged with the integration, testing, and operational maintenance of security within an organization. They take data from a variety of sources, aggregate and comb through it to find the essential meaning.

This intelligence-gathering characteristic sets security analysts apart from others in the organization. Not only must they possess deep technical skills, but they also must be aware of societal trends, stay current on geopolitics, and understand human behavior in order to predict a threat actor’s next move and how end-users should respond.

The need for more information security professionals with a higher level of management and intelligence capabilities doesn’t surprise Bill Stewart, a senior vice president with Booz Allen Hamilton. Stewart likens their role to that of an air traffic controller who must accurately track and predict activity so as to avoid congested runways or mid-air collisions.

In this case, the security analyst must be constantly aware of what’s happening inside and outside a network, and always remain one step ahead of threats to that network. “This role requires skills that bridge a variety of areas of expertise,” Stewart says. “More and more, the industry is moving toward creating intelligence and ‘hunt’ capabilities to find sophisticated adversaries within networks, pointing to a significant demand for staff with the security analyst skill set.”

This skill set also requires proficiency in areas not traditionally associated with technical fields.

In fact, two of the top three factors voted most important to an information security professional’s success were communications skills (91 percent) and a broad understanding of the security field (92 percent). Technical knowledge was third at 88 percent.

Deep technical know-how is important in any industry. A good CPA must know everything about accounting just as a good surgeon must possess outstanding surgical skills. But what makes them go from good to great is their ability to cull through disparate data to find meaning, to communicate with staff and clients, and to stay current on developments in their fields.

People seeking a thriving career in information security should strongly consider developing a higher order of management skills (traditionally considered to be outside the field). These skills include communications, policy formation and implementation, business and project management, and legal knowledge.

TAKE A LIFECYCLE APPROACH TO ADVANCED THREAT PROTECTION

Block, detect, analyze, and remediate advanced threats.
Discover how Advanced Threat Protection Lifecycle Defense enables you to protect your business from advanced threats, preserve your IT budget, and empower your users to embrace the very latest technologies.

LEARN MORE AT THE ATP RESOURCE CENTER: bluecoat.com/atplifecycle

© 2014 Blue Coat Systems, Inc. All rights reserved.
A new generation of threats is attacking your endpoints and servers—you need a modern defense.

If you don’t know what’s running on your systems, you should!

Start your Free Trial Today

bit9.com/freetrial

We are Bit9. The leader in advanced threat protection for endpoints and servers.

© 2014 Bit9, Inc.