



Using Security Metrics to Drive Action

33 Experts Share
How to Communicate
Security Program
Effectiveness to
Business Executives
and the Board



TABLE OF CONTENTS

Foreword4

Introduction5

Security Metrics That Tell a Story to the Board

Good Security Metrics Are a Work in Progress.....8

CEOs Require Security Metrics with a High-Level Focus.....10

To Lead as a CISO, Explain the Business
Impact of Security Risks.....12

Use Security Metrics to Present a Strong Action Plan.....14

Proactively Communicate the Right Security Metrics
—Before the CEO Asks.....17

Good Security Metrics Build Relationships and Trust.....19

Choose Security Metrics That Tell a Story.....23

Security Metrics That Help Boards Assess Risk

Security Metrics Should Show How Well
You're Adhering to a Plan.....28

Security Metrics Need to Show That Things Are Getting Done.....30

Security Metrics Help CEOs Balance the Cost of
Loss Against the Cost of Protection.....32

A Strategic Approach to Understanding and
Measuring Cybersecurity Risk.....34

To Be Thorough, Include Vendor Security Metrics.....37

Security Metrics Make Sense Only in the Context of Risk.....39

Define Security Metrics That Are Valuable Across the C-Suite.....41

Security Metrics Are About Illustrating Criticality vs Risk.....43

Security Metrics Need Validation and Context.....45

Present Security Metrics Using Risk-Based Language.....47

Security Metrics: It's a Composite Image.....49

TABLE OF CONTENTS

Security Metrics for Threat Management

With Security Metrics, Every Picture Tells a Story.....	55
With Security Metrics, You Don't Have to Sweat the Details.....	57
The Key: Linking Security Metrics to Business Objectives.....	60
Using Security Metrics to Defend the Business.....	62
Strengthen Security by Gathering Quality Threat Intelligence Metrics.....	65
Make Security Metrics Your Chaos Indicator.....	68
Government Agencies Rely Too Heavily on Compliance.....	70
Security Metrics Must Demonstrate Effective Security Governance.....	72
Security Metrics: The More You Know, the More You Grow.....	74

Security Metrics That Drive Action in the Financial Services Industry

The Best Security Metrics Are Actionable.....	78
Business Leaders Must Relate to Your Security Metrics.....	80
Communicating Security Takes More Than Raw Metrics.....	83
When It Comes to Security Metrics, Get S.M.A.R.T.....	85
For Financial Services, Security Means Trust.....	87

FOREWORD

Security has come a long way, but it continues to face two significant challenges: the continuous evolution and adaptation of attackers and the ongoing exposure to increasing and persistent threats that businesses face. IT security teams struggle to validate their ongoing security assurance efforts and justify budget requests to the board for managing risk and defending against threats. Metrics are an effective tool for both of these challenges.

Metrics help IT departments monitor current security controls and engage in strategic planning to determine where and how to implement new security controls. On their own, however, metrics can just be noise—easily overwhelming chief information security officers and confusing rather than clarifying the current state of organizational security. Therefore, it's important to collect the right metrics for the right reasons. The metrics you collect should have a direct, measurable impact and link security to business objectives.

This e-book illustrates the importance of actionable security metrics for businesses, both for operations and for strategy. The first-hand experiences collected here represent a diverse array of industries and perspectives that we hope will offer you valuable insight and best practices you can use as you implement actionable security metrics in your own organization.



Regards,
Ron Gula

CEO, Tenable Network Security



Tenable Network Security 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. Transform security with Tenable, the creators of Nessus and leaders in continuous monitoring, by visiting tenable.com.

INTRODUCTION

Your chief executive officer (CEO) is worried. He's spending more money on IT security. Even though he was assured that his latest IT security technology investments and policies are making the business safer, year after year, he sees organizations victimized by high-profile, costly breaches that severely damage business reputation and brand image. He's even seen some CEOs forced to resign because of their failure to protect customer data.

Security is a growing concern in the C suite, but conversations about security often leave executives unsatisfied and even confused. Why? Because the person responsible for implementing corporate security—the chief information security officer (CISO)—fails to discuss security in terms the other executives can understand. In fact, this “techno-gibberish” is typically why CISOs tend to be held in lower regard than other executives. We decided to find out how to help CISOs and other IT security leaders reduce their “geek speak” and talk more effectively about security to other C-level executives and the board. With the generous support of Tenable, we asked 33 leading IT security experts the following question:

Your CEO calls and asks, “Just how secure are we?” What strategies and metrics do you use to answer that question?

For anyone seeking a magic security metric that will dazzle CEOs and directors, you know that there's no one-size-fits-all metric. That said, the contributors to this e-book, based on their knowledge and experiences, believe that many security metrics are highly relevant to business strategy discussions. It's important to keep context in mind when choosing those metrics, but even the most relevant metrics need the right kind of presentation.

In this e-book, CISOs will discover metrics that support a wide variety of business situations and gain valuable insights that can strengthen their position in the C suite.



All the best,
David Rogelberg
Publisher

Mighty Guides

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.



How **secure** are you?

Without the proper tools to measure the security processes and functions in place within your organization, the answer to this question is typically just a “best guess”.



Download Now
Free Whitepaper

Read ***Communicating Security Program Effectiveness.***

Learn how SMART (Specific, Measurable, Actionable, Relevant, and Timely) security metrics and Tenable SecurityCenter Continuous View™ enables effective communication with business executives and the board.

Security Metrics That Tell a Story to the Board

In this Section...



Gary Hayslip
City of San Diego, CA.....8



Keyaan Williams
EC-Council.....17



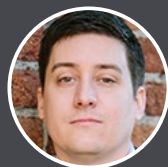
Ben Rothke
Nettitude Ltd.....10



Nikk Gilbert
ConocoPhillips.....20



Prasanna Ramakrishnan
Career Education Corporation.....12



Adam Ely
Bluebox Security.....23



David MacLeod
Welltok.....14

GOOD SECURITY METRICS ARE A WORK IN PROGRESS



**GARY
HAYSLIP**

Deputy Director/CISO
City of San Diego, CA

As CISO for the City of San Diego, California, Gary Hayslip advises the city's executive leadership, departments, and agencies on protecting city information and network resources. Gary oversees citywide cybersecurity strategy, the enterprise cybersecurity program, and compliance and risk assessment services. His mission includes creating a risk-aware culture that places high value on securing city information resources and protecting personal information entrusted to the City of San Diego.



Twitter | Website



Gary Hayslip found himself sitting next to the mayor of San Diego, California, one evening over dinner. The mayor turned to San Diego's chief information security officer (CISO) and asked, "Just how secure are our networks?"

'They are a work in progress,'" Hayslip responded.

It wasn't what the mayor wanted to hear, but it started the two on a half-hour conversation. In it, CISO Hayslip helped the mayor understand that cybersecurity is a life cycle, not an event. "And part of that life cycle," Hayslip explains, "is breaches. You never get 100 percent secure."

That's one reason why metrics are so important, Hayslip says.

"When you collect metrics, you're collecting them to tell a story," he states. "They have to be able to tell the story of your business." To that end, Hayslip keeps a sharp eye on three measurements:

- **Time to detect.** San Diego's networks average 66,000 attacks per day—22 million a year—that are successfully blocked, Hayslip indicates. It's inevitable that some attacks get through, he says. "My concern is, when they get in, how fast do I get alerts on them? How quickly do my firewalls and sensors detect that we've got an incident?"
- **Time to contain.** This metric allows Hayslip to know how quickly attacks are contained and cleaned up. Those numbers need to be examined carefully, however, he says. If incidents are contained in 20 minutes on average, that might seem fine, but if within that average some departments take as long as an hour, it might mean that some brainstorming is in order to find new security layers to protect remote or mobile assets.

“ When you collect metrics, you're collecting them to tell a story. ”

KEY LESSONS

- 1 Metrics are key for putting cybersecurity into a business perspective.
- 2 Use metrics to spell out your cybersecurity risks in hard dollar terms.



GOOD SECURITY METRICS ARE A WORK IN PROGRESS

- **Number of compromised systems.** San Diego hosts 14,000 desktop and laptop computers in its 40 departments, Hayslip notes. “So I have about 14,000 different doorways into my network.” On average, 45 machines are infected per month. By monitoring the number of compromises, he can gauge whether the city is staying within the acceptable exposure rate—for Hayslip, that’s about 1 percent of 10,000 machines per month. It also tells him whether he’s closing in on his personal goal of 10 machines per month. “That would be kind of phenomenal, when you look at the size of my network,” he adds.

These and other metrics—such as what types of attacks are getting through—tell Hayslip whether he’s succeeding in his overarching goal. “I want to be proactive,” he says. “I want to be able to see an attack before it infects the machine and to be able to stop it and kill it.” Metrics, in short, tell him how much work is yet to be done.

As it turns out, there’s still a fair amount of work to do, though much has been accomplished. Intrusions have fallen dramatically since Hayslip came on the scene, from a high of 160 intrusions per month down to 40. Phishing email attacks and infection from flash drives and websites are all down. Recently adapted cybersecurity technologies, including the Tenable Nessus agent scanner suite, have clearly been a big help, Hayslip asserts.

Not all metrics are created equal, of course. Hayslip used to monitor the number of help desk tickets that employees filed. That proved not terribly useful. “They could be submitting requests to my team’s email box that don’t even apply to us, just hoping someone is going to help them,” he explains.

In the end, Hayslip counsels CISOs to choose which metrics to track based not on their personal curiosity but on their business’ bottom line. “The metrics you collect need to mean something to the organization,” he says.

If possible, he concludes, tie metrics to hard dollars. He did that recently, showing city leaders that by replacing some vulnerable legacy technologies, the city could reduce direct financial risk by \$4.5 million and associated legal exposures by a whopping \$75 million. “That room was quiet,” Hayslip recalls. “Everyone was looking at us like, ‘Wow!’”

“

The metrics you collect need to mean something to the organization.

”

CEOS REQUIRE SECURITY METRICS WITH A HIGH-LEVEL FOCUS



**BEN
ROTHKE**

Senior eGRC Consultant
Nettitude Ltd.

Ben Rothke, CISSP PCI QSA, is a senior eGRC consultant with Nettitude Ltd. and has more than 15 years of industry experience in information security and privacy. His areas of expertise include risk management and mitigation, security and privacy regulatory issues, design and implementation of systems security, encryption, cryptography, and security policy development. He is a frequent speaker at industry conferences such as RSA and MISTI.

  
Twitter | Website | Blog

Chief executive officers (CEOs) just want to know that their systems are working and that important data are safe. “The CEO’s goal,” says Ben Rothke, “is to be in *The Wall Street Journal* because of record profits, not because of a data breach.”

In a CEO presentation, you may have 30 minutes to provide essential information about your security posture, with focused information related to an issue or a proposal. This is a time to provide metrics that really mean something to the CEO. What are those magic numbers? “When it comes to metrics, all numbers are the proverbial “it depends,”” says Rothke. Metrics need to effectively and clearly reflect the posture and the scenario under discussion.

It’s best to begin a presentation with a very brief overview of your security strategy. In this way, you put all your metrics and all issue-focused discussions into context. Rothke says, “You need to show you’ve got people, processes, and technology in place to make the firm secure.” This overview may touch on elements particularly important to the business or the issue at hand, such as physical security, security of third parties, application and end point security, and compliance with various regulatory standards. Then, you can dig into selected metrics to prove your points, always remembering that the CEO’s focus is high level.

“ The CEO’s goal is to be in *The Wall Street Journal* because of record profits, not because of a data breach. ”

KEY LESSONS

- 1 It’s important to understand that CEOs just want to know that their systems are working and important data are safe.
- 2 Be prepared for a discussion about what X dollars will buy in additional risk abatement and what the upside of that investment will be to the business.



CEOS REQUIRE SECURITY METRICS WITH A HIGH-LEVEL FOCUS

Several metrics Rothke finds useful under the right circumstances are:

- A baseline defense coverage metric, such as the percentage of devices that have some sort of defense, whether it be anti-malware, firewall coverage, intrusion prevention, or other relevant protections
- A systems-hardening metric and the percentage of devices or systems that meet a systems-hardening standard
- A patch management efficiency metric, which is an indicator of how quickly you respond to known vulnerabilities and the business' overall exposure at any given time.

“However,” explains Rothke, “when presenting any metric to the CEO, you should have a CEO-level reason for doing so, such as risk evaluation or the need to make a budget allocation decision.” For example, if the CEO becomes convinced that the company needs to have 100 percent of its systems patched within 72 hours, that will have a lot of implications. You have to consider whether such a task is even practical. What about salespeople who travel, will there be exceptions? You must be able to say, yes, that’s possible, but it will cost X dollars in additional staff and support engagement. You need to be prepared to have the discussion about what those X dollars will buy in additional risk abatement and what the upside to the business will be if you make that investment.

The higher you travel up the corporate chain, the more challenging it becomes to create meaningful security metrics. Security metrics are intimately tied to their underlying technologies, but the last thing the CEO cares about is technical details. Rothke says, “The CEO’s focus and his or her goal is ensuring that the company stays profitable.” According to Rothke, the most effective chief information security officers are those who have engineering degrees as well as an MBA. “They understand the depth and breadth and the technologies’ nuances, but they also know that in the context of business goals, the technology is really secondary.”



When presenting any metric to the CEO, you should have a CEO-level reason for doing so, such as risk evaluation or the need to make a budget allocation decision.



TO LEAD AS A CISO, EXPLAIN THE BUSINESS IMPACT OF SECURITY RISKS



**PRASANNA
RAMAKRISHNAN**

VP, Information
Risk Management
Career Education Corporation

Prasanna Ramakrishnan is VP of IT Risk Management at Career Education Corporation, where he is responsible for managing the strategy and operations for IT security policy, risk management, logical access, security operations and engineering, compliance and change control, and business continuity. Previously, Prasanna was the director of IT risk management at ULTA Salon, Cosmetics & Fragrance, leading all IT security and risk management activities while guiding the retail organization through all compliance challenges.

If the chief executive officer (CEO) were to call Prasanna Ramakrishnan and nervously ask, “How secure are we?”, his first answer would be, “Depends.” It’s not a simple black-and-white answer, he believes, and a chief information security officer (CISO) is best served by providing a cautious, nuanced approach to the CEO and the board rather than painting an overly rosy picture of security or risk management.

Traditionally, when describing the state of security to the CEO or the board, CISOs have always presented specific technology statistics—for example, vulnerabilities identified, patches applied, virus attacks spotted, and malware caught. Business executives rarely understand what those data points mean, however. “For example, if you say that you patched 3,732 vulnerabilities last month, what does that mean to a CEO?”, he asks. Ramakrishnan advises that CISOs focus instead on what kinds of security trends they are seeing at a high level so that executives can make informed business decisions.

For example, he says, “I would say that the trend we see is that we’re slow in reducing our lead time between identifying vulnerabilities and fixing them, and we need to speed that up.” When explaining why the security team is slow to fix vulnerabilities, this might mean sharing that they have been assigned other, conflicting priority projects that have taken up staff time, reducing the personnel available to address vulnerabilities. Recommendations for addressing that resource problem might involve automating a process or employing more people. Rather than talking about pure security statistics, this is the type of discussion that needs to happen with the CEO.

“ If you say you patched 3,732 vulnerabilities last month, what does that mean to a CEO? ”

KEY LESSONS

- 1 Rather than presenting metrics that the CEO or board may not understand, a CISO should explain security trends of importance to the company.
- 2 Visualizations such as infographics may aid in telling that story because they quickly capture executives’ attention.



TO LEAD AS A CISO, EXPLAIN THE BUSINESS IMPACT OF SECURITY RISKS

When talking about security trends, it's important to explain the impact to the organization. One useful way to do so is using comparisons or benchmarks, says Ramakrishnan. "It could be a vertical comparison, for example, saying that health care was the second-most highly targeted industry in America in the last quarter," he says. A CISO might note that trend and advise that because the business is in the health care sector, it might need to be more vigilant in taking preventative measures against possible attacks.

Presenting information in a form that's easy to consume and interpret is key, believes Ramakrishnan. "The challenge has always been to bring them to our level or same page of understanding, and I think that challenge has been there because we talk in numbers and they talk in words," he says. At his next board meeting, he plans to present the company's security information using an infographic. "The CEO and the board have limited time and attention, so you need to catch them quickly in that five minutes you get," he explains. "You may have a 30-minute presentation, but the 5 minutes is what they pay attention to."

Ramakrishnan observes that when CISOs simply read off stats about the number of vulnerabilities that exist or have been addressed, executives or board members may dismiss such data because they don't understand the potential impact on the business. CISOs should begin by telling a story, he feels, and visualizations such as infographics may aid in telling that story because they quickly capture executives' attention. Then, the discussion should transition toward identifying a trend and making the appropriate business decision in response to it. "Ultimately, the goal of sharing metrics is to make sure there's a follow-up discussion with the higher-ups to make an informed decision," Ramakrishnan explains.

By taking care to present a careful, nuanced approach using business language that tells a clear story, CISOs can help CEOs and board members make strategic decisions about business risks. Rather than focusing on sheer metrics and numbers whose meaning may not readily be understood, CISOs should identify trends, explain how they arose, and recommend specific courses of action to address them. This approach facilitates a meaningful dialogue at the top level, improving the organization's capacity for risk management and establishing the CISO as a true business leader.

“

Ultimately, the goal of sharing metrics is to make sure there's a follow-up discussion with the higher-ups to make an informed decision.

”

USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN



**DAVID
MACLEOD**

Vice President, CIO/CISO
Welltok

David MacLeod, Ph.D., FHIMSS, CISSP, CHS-III, and CISM, has been CISO for a large, multistate Blue Cross and Blue Shield organization; chaired the BCBCA Association Information Security Advisory Group; was CISO for a Medicare data center; and was appointed by Secretaries Thompson and Ridge to advise HHS and DHS on matters related to information protection and assurance in the health care and public health sectors as a part of the National Infrastructure Protection Plan and the federally sponsored Information Sharing and Analysis Centers.



Website

If the chief executive officer (CEO) asks, “Just how secure are we?”, David MacLeod says, “My answer focuses on how quickly I know that a breach occurred, what we’ve done to ensure that the alarms will go off when they should, that we’re alerted when any kind of an anomaly happens that could possibly be an incident that is either security or privacy related, and that we have planned in advance how we are going to respond.”

He stresses that it’s important to give the CEO confidence that the security team has made the appropriate plans, knows what measures to take in the event of an incident, and is clear on how to respond immediately when it takes place. “That’s how they’ll know how secure we really are, because it is not a question of if, but rather of when a malicious event will occur – and how we will respond to it,” he says.

When it comes to metrics, MacLeod likes to provide information about how many malicious events have been detected and either prevented, or responded to. As an example, his team reports on the volume of malicious emails his team blocks and filters, including spam. “They’re always impressed to hear that we receive 2.5 million emails a month and, out of those, about 12 percent are actually valid and allowed into the organization,” he notes.

“That’s how they’ll know how secure we really are, because it is not a question of if, but rather of when a malicious event will occur.”

KEY LESSONS

- 1 When presenting security metrics to the CEO or board, a CISO should give them confidence that a strong action plan for responding to incidents is in place.
- 2 The human element of information security is also important to highlight, so it’s wise to share metrics on security awareness training.



USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN

At his organization, which is in the health care sector, privacy is of particular importance. Accordingly, the board especially likes to hear about the number of outbound emails that contain protected information that their system automatically captured and made sure were delivered securely instead of being transmitted over an open email communication.

MacLeod also shares statistics on activities taking place at the electronic perimeter. “I can tell them that this month there were more than a million incidents at our firewalls. They ranged from innocuous suspicious activity to actual attempts to see if there was a vulnerability that could be exploited to get into our systems,” he says. To help the board understand the potential impact of these trends, he uses an analogy. “I say that some of these activities are like people looking at your house to see if there’s a window or door left open versus an actual attempt where someone would be coming up and actually trying to open a window or a door,” he offers. By putting security metrics into a commonly understood context, his C suite peers and the members of the Board can better relate to and understand these metrics.

The human component of security is also important to highlight, so MacLeod presents statistics around people and their level of security awareness. “We have an active security awareness campaign on which I provide the board with statistics so that they know what we’re doing to keep our workforce informed. This way, we can make sure that they’re looking at things from a security or privacy perspective,” he says. MacLeod shares data ranging from the relative strength of passwords employed by the workforce to how many people have completed his security awareness training, how many haven’t, and how many people require more assertive follow-up to ensure their participation.

MacLeod’s team spends a lot of time sending out security alerts to the company’s workforce warning them about some of the scams the Internal Revenue Service has been reporting on, for example. “If I can get them to think about protecting their personal information, it’s easy to get them to care about protecting company information,” he says.



We have an active security awareness campaign on which I provide the board with statistics so that they know what we’re doing to keep our workforce informed.



USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN

“We don’t just worry about telling them how to protect the company assets. We want them to always think about things with a mind on security, privacy, and protection of information—no matter who information belongs to.” With so many employees working from home or telecommuting, using their own equipment and network to access company resources, this awareness becomes even more crucial.

Above all, MacLeod emphasizes, it’s important to demonstrate to the CEO and board that the CISO has assessed the threats facing the company and has a clear action plan in place for responding to an incident should it occur. This way, leadership can understand the company’s current state of security preparedness as well as the CISO’s strong leadership position in proactively assessing and responding to risks as they emerge.

“

If I can get them to think about protecting their personal information, it's easy to get them to care about protecting company information.

”



KEYAAN WILLIAMS

Senior Executive,
CCSIO Programs
EC-Council

Keyaan Williams has dedicated more than 15 years to the information security profession as a leader, educator, and volunteer. He has experience developing security programs and strategies for critical infrastructure, high-security systems, and business IT systems. He currently serves as the senior executive for the Certified CISO Program at the EC-Council and remains active in the information security industry, serving in board and advisory positions for ISSA International, Metro Atlanta ISSA, ISSA the CISO Advisory Council, and the SecureWorld Atlanta Advisory Board.



Twitter | Website



Keyaan Williams thinks that a chief information security officer (CISO) who has been in the position longer than 90 days should never receive a nervous call from the chief executive officer about business security. The question should already be answered.

Communication is a key aspect of effective leadership, Williams explains. Part of the CISO's role is to define and communicate security strategy, then get everyone to buy in. Metrics play a key role in that effective communication, Williams says.

Conversely, he adds, "The way you develop your security strategy and align it to the business influences what kind of metrics you're going to gather." Therefore, if he had to choose three key metrics to focus on, Williams says it would be these:

- **Access control.** How often, through what means, and when are people accessing your network? These metrics show whether you are effectively preventing unauthorized network access while allowing reasonable and authorized access. "Is there some kind of anomaly?" he asks. "Is there an administrator logging on in the middle of the night for some reason that makes no sense?" Be smart and flexible in responding to these metrics, however. If a particular data modeler tends to log on in the middle of the night to work out solutions, you should be able to spot that trend.

“The way you develop your security strategy and align it to the business influences what kind of metrics you're going to gather.”

KEY LESSONS

- 1 Effective communication of security information—before the CEO asks—is a measure of a CISO's effectiveness.
- 2 Be intelligently selective about metrics: focus only on those that provide business value.



You don't want to block that kind of productive activity. Of course, if you see that someone has tried and failed to log on 700 times, you might want to call on your rapid response team.

- **Incident volume.** You can learn a lot from the raw number of security incidents, including simple virus infections, Williams counsels. At a previous job, he measured the number of such incidents by corporate division. Where intrusions happened repeatedly to specific users or groups, retraining was conducted. If the same users later had even more repeat incidents, it could be determined whether they either were not following instructions or the training itself was flawed. "If we measure the number of incidents, then we can make correlations—tie the incidents to specific users, environments, and areas within the organization," Williams says. "That can then allow us to do further evaluation or investigation."
- **Physical access.** This much-neglected metric can be highly productive, Williams says. Employees, particularly in high-security areas, often must wear smart badges and radio-frequency identification monitors to access security-sensitive areas. Visitors must often be accompanied on walkthroughs and sign in each time they access higher-security zones. They pass closed-circuit television monitors. Measurable, quantifiable data can be captured from those sources and other forms of multivector authentication. Physical access is a subject many CISOs overlook—at their own peril. "Everything that we do from a digital security perspective has its roots in physical security," Williams notes.

Whether you follow Williams' specific advice or not, the point is to be intelligently selective. Follow the metrics that are most important to your particular business. Don't waste your time on pointless measurements. In a previous CISO job, for instance, Williams was required to monitor Microsoft SharePoint server accesses. Nothing was ever done with the information—a total waste of time and resources.

“

We are using the metrics to actually tell the story of how effective our controls are.

”



PROACTIVELY COMMUNICATE THE RIGHT SECURITY METRICS—BEFORE THE CEO ASKS

Effective monitoring of key metrics not only helps detect security patterns and trends as well as spare your business needless disruption, but it also communicates to executives that your office is on the ball. That, obviously, can help keep your CISO office budget afloat so you can be even more effective in safeguarding company security, Williams says.

“We are using the metrics to actually tell the story of how effective our controls are,” he says, “and more importantly, those that identify where controls are not effective so that we can take corrective action. We are making that justification based on what we have measured.”

“

If we measure the number of incidents, then we can make correlations—tie the incidents to specific users, environments, and areas within the organization.

”

GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST



**NIKK
GILBERT**

Director of Global Information
Protection and Assurance
ConocoPhillips

Nikk Gilbert has 18 years of executive-level experience in the government and private sectors and is a respected information security leader. Currently the director of information security for ConocoPhillips, he's a Distinguished Fellow of the Ponemon Institute, a recipient of the US Navy Meritorious Civilian Service Medal, and a frequent speaker at technology events throughout the world.



Twitter | Website | Blog



For Nikk Gilbert, the secret sauce to success as a chief information security officer (CISO) is forging relationships. Metrics, he says, can be a great way to solidify those relationships.

Rather than advising readers to select a group of generalized metrics to monitor, Gilbert prefers to tell a story. Metrics, after all, are designed to tell the story of how well you're succeeding at digitally securing your enterprise.

After starting work at a previous company, Gilbert avoided making aggressive changes to the way security was handled. Instead, he took co-workers out to lunch, one at a time. Some panicked—what does the CISO want? Did I do something wrong? It wasn't about that, Gilbert says. "Quite frankly, I sat there and talked to them about everything but security," he states. "It was creating the relationships."

After establishing himself as an approachable leader, it was easier to talk about changes that needed to be made to protect customer data, intellectual property, and other proprietary information from malicious outsiders. During this process it was important to avoid drowning people in metrics.

“ 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. ”

KEY LESSONS

- 1 Metrics can be a great way to establish the CISO's integrity within the enterprise.
- 2 Measuring metrics, both at the operational and strategic levels, is vital.



GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST

“There are so many metrics out there that you can use to show different things,” he says. “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.”

Right around the same time, Gilbert’s team created a real-time online dashboard to monitor internal networking metrics. He used it to show key team members the value of monitoring several operations-level metrics, including:

- **Web proxies.** This software allows authorized employees to surf authorized websites while blocking risky sites. “It’s a tool that helps us protect users from themselves,” Gilbert states.
- **Admin account accesses.** Administrative accounts are extremely sensitive. “We have a real-time dashboard that watches access to admin accounts,” he says. If someone tries over and over to access an account unsuccessfully, the account gets flagged and additional actions can be taken as appropriate.
- **Data in/data out.** The dashboard has a plug-in that reveals how much data is moving in and out of the network and through which ports—crucial information that can reveal whether, say, a denial-of-service attack is beginning.
- **Antivirus activity.** If a computer is infected, the dashboard throws up an antivirus alert.
- **Firewall alerts.** The dashboard monitors the network firewall’s sensors, which can detect a variety of network based indicators.

Individually, Gilbert acknowledges, there’s nothing spectacular about these metrics, but holistically, they demonstrate how it’s possible to use resources to respond to the metrics and stop an attack from grinding the business to a halt. They also help reveal which resources were still lacking. “That’s when we became invaluable to the executive team,” he notes.

“

It was a really good moment for that executive buy-in we're all looking for.

”



GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST

When his chief information officer (CIO) saw the dashboard for the first time, he was, in Gilbert's words, "knocked off his feet." The CIO was big data oriented, Gilbert explains, and he immediately saw ways to tie the dashboard's metrics into further big data analysis to extrapolate even more insights. "It was a really good moment for that executive buy-in we're all looking for," Gilbert says.

What's more, because he had carefully established rapport with the crew, coworkers had confidence in Gilbert and his team. In other words, they trusted his metrics.

The moral of his story, Gilbert says, is that the CISO needs to understand how to simply and effectively communicate security metrics. When you secure the support of the team, it is then crucial to continue showing the value of your security program. Measuring metrics, both at the operational and strategic levels, is vital to that task.

As a final note, he adds, keep your audience in mind. One size does not fit all when it comes to relating the security story within your enterprise. "Executives don't want to hear about servers, and the security analysts don't want to talk to the executives," Gilbert says. "So I guess I'm a universal translator."

“

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.

”

CHOOSE SECURITY METRICS THAT TELL A STORY



**ADAM
ELY**

CSO and Co-founder
Bluebox Security

Adam Ely is the co-founder of Bluebox Security. Before that, he was the CISO of Salesforce.com's Heroku business unit, led security and compliance at TiVo, and held security leadership roles within The Walt Disney Company, where he was responsible for the security of such Web properties as ABC.com, ESPN.com, and Disney.com. Adam also advises technology companies and has been a contributing author to *Dark Reading* and *InformationWeek*. He holds CISSP, CISA, and NSA IAM certifications and received an MBA from Florida State University.



Twitter | Website



Adam Ely had spent most of his career as a chief information security officer. Then, he started a security company and found himself in the position of being the person to whom he used to report. The change has given him a new perspective on which security metrics are really useful to the C suite. "Generally, chief executive officers, chief operations officers, and other business line executives are inundated with data from all the departments that report to them. Giving them the wrong metrics is usually just noise that they're not going to be able to comprehend and understand quickly."

A better approach, according to Ely, is to present metrics that tell executives a story. "Hopefully, I'm already prepared for that call," he says. "Hopefully, I already have an answer and can educate them more on where the gaps are by using metrics. I would look at data around probabilities of compromise, and specifically I would look at where have we had issues in the past quarter or two. Where do I believe that our security programs are underperforming?"

Ely says, "I'm looking for any indicator that tells me that we're progressing or slipping. Then, I'm going to use those things along with metrics from the industry to understand what constitutes the norm and what we can expect." He uses this information to build a full answer to take to the C suite that provides solid, quantifiable information about how the organization is getting better over time.

“ Look at data around probabilities of compromise and specifically at where issues occurred in the past. ”

KEY LESSONS

- 1 Stay away from tactile metrics that don't help executives understand the value of the security program.
- 2 Use metrics to build a cohesive story that illustrates the probability of security issues, the potential damage that can be done, and steps necessary to reduce those risks.

CHOOSE SECURITY METRICS THAT TELL A STORY

“Or we’re not. Whatever the answer is,” says Ely. “Here’s the area that we really need to focus on, and here’s the level of effort we need to apply. It’s about connecting the dots.”

One way to connect those dots is to select metrics that help illustrate the current state of security within the organization, including specific needs like investments or personnel. Then, define the overall value of those needs as they apply to the rest of the organization.

Ely says, “It’s not that executives don’t care about security. It’s that they have a lot of things to care about, and the people who articulate their area’s value proposition the best are those who get the most mindshare and the most resources. So, the value of security metrics is not to say, ‘We have patched a hundred servers and we still have to patch another hundred thousand servers.’ It’s to say, ‘We have this probability of getting broken into; that’s going to lead to an operational cost of \$500,000. If data are stolen, that’s going to lead to a cost of \$14 million. And there’s a 76 percent likelihood that this will actually happen.’ It’s all about driving it back to the mission of the business, the betterment of the business, and ultimately—in many cases—the dollars associated.”

To really hone in on the metrics that will help you illustrate this story of security, Ely says it’s best to stay away from certain metrics that have little meaning to executives. “Any metrics that are day-to-day operations–type metrics aren’t worth looking at. Executives care about the big picture, but anything that’s low level and tactical just doesn’t have enough meaning. Roll that information into a larger story that has more value and more meaning behind it.”

“Build a cohesive story that people can understand,” says Ely. “Raw metrics are valuable from an operations standpoint, but at the executive level, it’s about a cohesive story that helps executives understand the value of the security program and keeps the company moving forward.”

“

Raw metrics are valuable from an operations standpoint, but at the executive level, it's about a cohesive story.

”



How Confident Are You in the Effectiveness of Your Security?

In a new 2016 survey, global cybersecurity readiness earned a score of just 76%, or a "C" average.



Download Now
Free Whitepaper

Read **2016 Cybersecurity Assurance Report Card.**

Benchmark your organization and security practices with those of your peers. Obtain key insights on how you can improve your ability to assess and mitigate network security risks.

Security Metrics That Help Boards Assess Risk

In this Section...



Tim Prendergast
Evident.io.....28



Robin "Montana" Williams
ISACA.....34



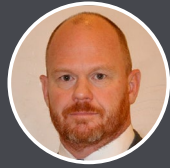
Charles Tholen
Cognoscape LLC.....30



Jake Kouns
Risk Based Security.....37



Daniel Riedel
New Context.....32



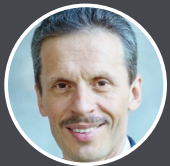
Chris Mark.....39



Andrew Storms
New Context.....41



Scott Singer
PaR Systems, Inc.....47



Genady Vishnevetsky
Stewart Title Guarantee
Company.....43



Roy Mellinger
Anthem, Inc.....49



Trevor Hawthorn
Wombat Security
Technologies.....45

SECURITY METRICS SHOULD SHOW HOW WELL YOU'RE ADHERING TO A PLAN



**TIM
PRENDERGAST**
CEO
Evident.io

Tim Prendergast is founder and CEO of Evident.io. He has always pushed the limits of technology, creating Evident.io as the first security company focused solely on programmatic infrastructures (cloud). His prior experience includes leading technology teams at Adobe, Ingenuity, Ticketmaster, and McAfee. He has more than 15 years of security experience, including 8 in Amazon Web Services (AWS) security experience and 3 in the Adobe AWS infrastructure, from inception to production.

  
Twitter | Website | Blog

Security metrics that matter to the chief executive officer (CEO) depend on a lot of variables, including the organization's maturity. "If we answer this question from the perspective of a mature organization," says Tim Prendergast, "there are two high level questions the CEO wants answered: Is our security getting better or worse? and are we adhering to our security strategy?"

One way to answer the first question is to see how you perform on a variety of assessments over time. A key metric is the frequency of execution against a risk and assessment plan—in other words, how often you run vulnerability and risk assessments, how often you run penetration tests, and the overall trend of the results of those tests. If you see increasingly better results each time you run the tests, then you know you have an effective security program that is reducing your attack surface and your scope of vulnerability. "But if those examinations discover more issues over time, your security practice is most likely drifting in the wrong direction," says Prendergast.

Determining how well you're adhering to your security plan is a little more difficult. One metric you can use for this purpose is how many new products and new technologies you have released into the environment in the past 12 months and how many breaches have been associated with those products.

“ There are two high level questions the CEO wants answered: Is our security getting better or worse? and are we adhering to our security strategy? ”

KEY LESSONS

- 1 If you see better results each time you run the tests, you know you have an effective security program that is reducing your attack surface.
- 2 Metrics that measure the security IQ of people accessing your cloud environments are a good place to start.

SECURITY METRICS SHOULD SHOW HOW WELL YOU'RE ADHERING TO A PLAN

Prendergast says, "That gives you a good idea of how well the company is doing at deploying new technology in adherence with the corporate security requirements." An effective IT security practice will strive to release new technology that is secure, which minimizes the time it needs to spend fixing things later.

Measuring the security of cloud-based assets and assessing cloud service providers are growing challenges for many companies for several reasons. One is that more products and services are cloud-based, so a threat to cloud-based assets is a direct threat to the viability of that business. Another reason cloud security has become so important is that employees routinely set up cloud resources and move assets into the cloud. "It used to be that a few people controlled access policies, managed all the firewalls, and controlled security for the company," explains Prendergast. "Nothing ever changed unless it went through those few people." That's all different now. Now, you have thousands of developers in an organization who control and manipulate cloud environments.

So, which metrics can you use to show the security of your cloud resources? Metrics that measure the security IQ of people manipulating those cloud environments would be a good place to start. For instance, you can show the percentage of your developers who went through a cloud security training program and showed proficiency in your cloud security policies. This also becomes an enablement strategy. "You're telling your developers that they can do things as long as they run the right technologies and follow policies."

A tougher issue for many businesses is evaluating the security posture of their third-party cloud vendors. Several metrics can help with that. One is to look at a provider's service-level commitments; another is to look at the number of compliance certifications the provider holds for its infrastructure and which cloud services it covers. It's also important to look at how well your vendors maintain those certifications, how many different certifications they have, and whether those certifications are relevant to your industry. "A report card on the security posture of your partners is a critical metric you should track continuously," says Prendergast.

“

A report card on the security posture of your partners is a critical metric you should track continuously.

”

SECURITY METRICS NEED TO SHOW THAT THINGS ARE GETTING DONE



**CHARLES
THOLEN**

Owner and CEO
Cognoscape LLC

Charles Tholen is an entrepreneur and founder of Cognoscape, a business technology company that specializes in bringing enterprise-class technology solutions to small and medium-sized businesses. Cognoscape is a fast-growing managed IT service and managed security service provider that has expertise in the legal, health care, financial services, and professional services verticals. Charles is a seasoned technologist, with broad experience with authentication, disaster recovery, antivirus, systems management, and security management in Fortune 500 enterprises.



Twitter | Website | Blog



There's no simple answer to "How secure are we?". The answer invariably depends on the maturity of an organization's approach to its security strategy. Companies need to establish a baseline measure of their security posture so that they can see how that baseline changes over time. "We do a baseline assessment, which gives a weighted scoring of 0 percent to 100 percent on where we are with different functional and technical areas," explains Charles Tholen. "Then, we can provide follow-on reports either after significant events or on a periodic basis."

A baseline assessment begins with identifying data assets essential to the business, the technical infrastructure and environment where the data reside, and each type of data and where those types are located. The assessment also reviews rules of data governance and procedures for risk assessment and management.

As a company develops and implements its security program, it must also develop metrics that provide visibility into the effectiveness of that program. For example, if compliance is important to the company, there must be a metric, such as a percentage compliance number or a compliance gap metric, that indicates where you stand with regard to compliance standards.

“ The CEO wants to know whether a process is or is not implemented and if not, where in the implementation cycle it is. ”

KEY LESSONS

- 1 Metrics that are most useful to the CEO relate to how far along the program is in achieving its goals.
- 2 Security is more than just an operational cost. It's also increasingly becoming a business enabler.



SECURITY METRICS NEED TO SHOW THAT THINGS ARE GETTING DONE

Or, if patch management is an important part of the strategy, there should be a metric that shows how effectively the company handles known vulnerabilities. This might be a percentage of vulnerabilities outstanding at any given point in time, a time-to-patch metric, or a combination of these two. Several metrics and performance indicators relate to key aspects of a company's security strategy. "How secure you are is represented by metrics associated with goals in key areas of your security program," says Tholen.

While this information is an integral part of any security program, these metrics are not necessarily what a Chief Executive Officer (CEO) wants to hear. "A CEO doesn't care that under your vulnerability management program you have 80 percent of your vulnerabilities remediated this week," says Tholen. "He or she wants to know whether a process is or is not implemented and if not, where in the implementation cycle it is." Metrics that are most useful to Management relate to the success and progress of the program. In short - the CEO really wants to know that it's getting done.

It's also important to associate CEO-level security metrics with the cost impact on the organization. "It's one thing to say there's a system vulnerability, but that means nothing without a price tag associated with the risk," says Tholen. Analyzing the dollar impact draws a perspective that is meaningful to the CEO. This perspective rationalizes security expenditures and prioritizes the vulnerability management program. Identifying the cost impact also becomes a fundamental planning element when appropriately allocating resources and investments as you work to mitigate ongoing operational risks.

Executive management's attitude toward security is changing. One clear reason is the importance of data to daily operations and the growing risks associated with losing those data. Another factor is the increased responsibility placed on the shoulders of executives regarding the integrity of their data security and potential breaches. Beyond that, is the realization that security is more than just an operational cost. It's also increasingly becoming a business enabler. "Proving a strong security posture can provide a competitive advantage," Tholen says. In certain situations, security metrics can be framed in the context of pursuing and winning new business opportunities, and that discussion will be of great interest to the CEO.

“

It's one thing to say there's a system vulnerability, but that means nothing without a price tag associated with the risk.

”



**DANIEL
RIEDEL**
CEO
New Context

Daniel Riedel is the CEO of New Context, a systems architecture firm founded to optimize, secure, and scale enterprises. New Context provides systems automation, cloud orchestration, and data assurance through software solutions and consulting. Daniel has experience in engineering, operations, analytics, and product development. Before New Context, he had founded a variety of ventures that worked with companies such as Disney, AT&T, and the National Science Foundation.

  
Twitter | Website | Blog

Enterprise IT environments can have thousands of people trying to do the same thing at the same time. These IT environments are driven by thousands of applications that are continuously built and deployed into the environment. A huge number of metrics are used to measure all this activity. “This is a problem for the industry right now: knowing which key metrics a business should use to make strategic security decisions,” says Daniel Riedel.

Most security professionals use a core set of metrics such as numbers of intrusions, time to resolution, and trend data to assess their systems, but the significance of these metrics can vary greatly depending on the type of business and its level of IT maturity. Ultimately, it all has to be communicated upward to the chief executive officer (CEO) and board of directors. “The challenge for many security professionals is that the board has to make financial decisions,” says Riedel.

As Riedel explains, “Measuring and quantifying the organizational awareness of risk are essential for managers and decision makers.” Although every business will take its own approach to this kind of metric, Riedel believes that all businesses can benefit from a financial analysis of risk awareness. This means looking at risk from two perspectives:

“ This is a problem for the industry right now: knowing which key metrics a business should use to make strategic security decisions. ”

KEY LESSONS

- 1 Risk-cost awareness provides guidance on how to allocate resources to secure the enterprise infrastructure.**
- 2 With risk-cost awareness, it's possible to communicate security metrics to the CEO or board in terms that enable them to make the necessary financial decisions.**



- **The value of your data to potential thieves.** This is an indication of how much effort thieves will devote to trying to steal your data.
- **The value of your data to your own business.** This is really a measure of the cost of a data breach to the business. It can include costs of total data loss, costs of remediation, damage to business operations, damage to brand, lost revenue, lost opportunity, fines, lawsuits, and other kinds of costs.

“These assessments may vary from one business unit to another within the enterprise,” says Riedel, “so CEOs need to ask all their reports to provide this kind of value metric.”

At a high level, these data provide guidance on how to allocate resources to secure the enterprise infrastructure. For example, if you have a \$100 million company and the worst-case total cost of a catastrophic breach is \$10 million, this gives you an idea of how much you should spend to protect those data. In contrast, if you have a \$100 million company and your total risk liability is \$100 million or more, you’re looking at a bankruptcy risk, and that suggests a different level of security investment.

“When you have this overall risk awareness,” explains Riedel, “then you use more granular security metrics to break down risk components and costs of protection.” For instance, in a worst-case scenario, what are the contributors to the damage? Is it loss of operations, brand damage, or costs of recovery and remediation? What are the risk factors specific to each of those elements? What are the specific, quantifiable vulnerabilities in each of these risk factors? In that way, the right granular security metrics can roll back up to the CEO or board in terms that enable them to make the necessary financial decisions.

Riedel says, “This is also how security professionals can make a case for the most cost-effective applications of resources to offset those vulnerabilities.” For example, does it make more sense to invest in more peripheral security, or is it better to spend on building security into DevOps processes that result in more secure code for business operations? “Mapping granular security metrics back to risk–cost assessments help decision makers answer those questions,” says Riedel.

“

Measuring and quantifying the organizational awareness of risk are essential for managers and decision makers.

”



ROBIN "MONTANA" WILLIAMS

Senior Manager, Cybersecurity Practices & Cyber Evangelist
ISACA

Robin "Montana" Williams is ISACA's senior manager, Cybersecurity Practices & Cyber Evangelist. His team executes ISACA's cybersecurity strategy, and he manages Cybersecurity Nexus, the industry's first performance-based certification and professional development program. Montana served as chief of DHS' Cybersecurity Education & Awareness Branch, was a senior White House advisor for the National Initiative for Cybersecurity Education, and helped architect the National Cybersecurity Workforce Framework.



Twitter | Website



When the chief executive officer (CEO) asks you, "How much cybersecurity do we need?" Montana Williams believes the answer begins with conducting an assessment that outlines the organization's current cybersecurity strengths, weaknesses, opportunities, and threats. According to Williams, a cybersecurity evangelist who has deep experience in the field, it's important to identify the technical, human, and financial resources you currently have. Then, you should develop organizational goals that follow the SMART model—that is, they should be *specific, measurable, achievable, realistic, and timely*.

After you have completed an initial assessment and defined your organization's goals, you can develop a reporting process that measures your progress. "One effective method for communicating the state of your cybersecurity to the CEO is a dashboard," Williams says. It should show the organization's current level of vulnerability; display metrics on threats that have been detected, such as how many phishing messages have been intercepted and what percentage of vulnerabilities have been mitigated within a prescribed period of time; and provide updates on other key security metrics of importance to your organization.

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

KEY LESSONS

- 1 To determine which security metrics are important to measure, you must first understand your risks and define goals for addressing them.
- 2 The human aspect of cybersecurity risk management, including awareness training and policy compliance, is especially important to measure and monitor.



You may also need to measure compliance, depending on the type of organization you're in. Health services organizations are often subject to Health Insurance Portability and Accountability Act (HIPAA) rules, for example, and financial institutions must observe US Securities and Exchange Commission requirements.

Performance effectiveness is also important. How often is your network down? What percentage of your devices are fully updated with the right software? Physical security violations, such as the number of incidents involving unauthorized people accessing the facility or the number of times employees violated the clean desk policy, should also be tracked.

The human aspect of cybersecurity is critical to your success but easy to overlook. Says Williams, "Measure whether your people are properly trained and following the proper cybersecurity procedures." Also note the number of people who have received updated cybersecurity training, the percentage of your staff who have current technical certifications, and the number of users who have been granted elevated privileges on your network.

When assessing value, ask yourself, "What's the value of the information that my organization holds? What does it mean to me, and how much is that intellectual property or customer data worth?" Also consider how much it would cost to replace that information in the case of loss, tampering, or destruction.

Consider the cost of regulatory fines, as well. If you do something wrong and receive a fine for a HIPAA violation, what is that going to cost you? Take care to calculate and measure your risk exposure. Metrics in this category might include the types of risk exposure and threats you face, who's attacking you, how exposed you are, and how big a target you might be.

“

Measure whether your people are properly trained and following the proper cybersecurity procedures.

”



As for measurements to skip, Williams advises that organizations pass on tracking the number of authorized changes that occur on their networks, which is something that can already be noted as part of a change management process. He says that, from a cybersecurity standpoint, it's important to make changes when they are necessary. It's also not as important to measure where the attacks are coming from: "You can solve 90 percent of your problems with good patching, good training, and being aware of what your adversary might want."

By performing a careful risk assessment and outlining a path to addressing your organization's risk in the form of goals and objectives, you will have a strategic roadmap that can inform the metrics you need to establish. With clear shared goals in place, you can measure them and mark your progress toward improving your overall cybersecurity resilience in terms that everyone, including the board, can understand.

“

You can solve 90 percent of your problems with good patching, good training, and being aware of what your adversary might want.

”

TO BE THOROUGH, INCLUDE VENDOR SECURITY METRICS



**JAKE
KOUNS**

CISO
Risk Based Security

Jake Kouns is the CISO for Risk Based Security and has presented at many well-known security conferences, including RSA, Black Hat, DEF CON, CanSecWest, DerbyCon, SOURCE, FIRST, and SyScan. He is the co-author of the books *Information Technology Risk Management in Enterprise Environments* and *The Chief Information Security Officer*. He holds an MBA, with a concentration in information security, from James Madison University.

  
Twitter | Website | Blog

Jake Kouns believes that there's a different kind of security metric executives should look at more closely. Most medium-sized and large organizations focus on securing their infrastructure. They have a solid foundation for measuring and understanding their security posture. "I think many people say, 'Our front door is locked and now we're safe.' I say to them, 'But what about all your vendors?'"

Security is complicated. There's a long list of things you need to do well to have a solid security posture. With companies depending more and more on outsourced software products, cloud-based services, and partner relationships, those connections become potential vulnerabilities. "Anytime I become aware of credentials that are part of my domain," says Kouns, "I want to take early action to secure that access point."

Many companies do a poor job of measuring the risk that vendor relationships pose. If the potential cost of a breach is high, it may be worth changing the company's mix of vendors and partners. Those risks must be understood and balanced against other factors when weighing the value of strategic business relationships. Chief executive officers (CEOs) need to understand vendor and product risks from a business decision-making perspective. As Kouns explains, "Most CEOs and people with purchasing power for these products and services don't understand the technical metrics."

“ Many people say, ‘Our front door is locked and now we're safe.’ I say to them, ‘But what about all your vendors?’ ”

KEY LESSONS

- 1 With companies depending more and more on outsourced software products, cloud-based services, and partner relationships, those connections become potential vulnerabilities.
- 2 CEOs need to understand vendor and product risks from a business decision-making perspective.



TO BE THOROUGH, INCLUDE VENDOR SECURITY METRICS

Kouns uses a five-star vendor rating system based on several calculations:

- One key calculation is called *Vulnerability, Timeline, and Exposure Metrics* (VTEM). It looks at the vulnerability life cycle in the context of a specific vendor or service, from the time a vulnerability is introduced into the code to the time someone finds it to the time someone informs the vendor to the time the vendor responds to that researcher to the time an exploit comes out to the time a solution is developed and finally to when the organization corrects that issue through a patch or some other means. "If you think about that," says Kouns, "that is your total time of exposure, from the minute it happens until you correct it." Several calculations based on these metrics can show whether a vendor actually cares about security and is correcting things in a timely fashion.
- Another assessment looks at the organization's "cyber-hygiene" as a whole based on breaches. If a company is subject to regular breaches, the probability is high that it will be breached again. Other factors come into play here, as well, such as who the organization is, its size, the kind of data it handles, and the kinds of partners and customers it has.

Combining VTEM and breach metrics into a simple rating system gives a good indication of how vendors handle security for their products and services. This becomes important to any company that uses those products and services. If the chief executive officer (CEO) calls, the chief information security officer can say that the company has a solid security program in place, and a key piece of that is working with vendors that care about the security of their products and services. "In that conversation," says Kouns, "I can say, 'Here's our scorecard, and you can see the ones that are doing well and the ones that are not.'" The CEO can then be involved in the discussion about what's behind a poor security rating for a particular vendor that might be important to the company and how to improve the company's security by either dealing with or replacing the vendor.

“

Anytime I become aware of credentials that are part of my domain, I want to take early action to secure that access point.

”

SECURITY METRICS MAKE SENSE ONLY IN THE CONTEXT OF RISK



**CHRIS
MARK**

Chris is a risk management & security expert with over 20 years of experience in physical, maritime, operational and information security. He has extensive experience in the payment card industry, has published scores of security articles, and has spoken at over 100 events worldwide. Chris has a BA, MBA, and is pursuing a doctorate in information assurance. He is a combat veteran of Operation Continue Hope and has served as a Marine Scout/Sniper & Force Reconnaissance Marine as well as a US Navy Officer.



Security is not a binary proposition of being either 'secure' or 'not secure'. Chris Mark likes to use his house as an example. "Is my house secure?" he asks. "I have locks on my doors and windows. I believe it is *appropriately* secure given the identified risks against which it is being secured. But if I were to bring the Hope Diamond into my living room, that level of security would no longer be considered appropriate given the new risk profile." The question of how secure we really are can be answered only in the context of identified risk. "When talking about security metrics, the first step involves conducting a risk analysis," says Mark. "You need to be able to say that given the threats facing your organization; the value of your data; and the operational, regulatory, financial, and safety impacts of a breach, here is the appropriate level of security given the identified risks to which you are exposed."

With a risk analysis in hand, you then have many metrics that can illuminate your security posture to see if it meets your requirements. When presenting to the chief executive officer (CEO) or board, you must select metrics that:

- Show that you have conducted a rigorous risk assessment;
- Describe an appropriate level of security to address possible threats and necessary controls that are commensurate with your risk profile;
- Show your compliance standing;

“ As important as compliance is, being compliant does not equate to being secure. ”

KEY LESSONS

- 1 The question of 'how secure are we' can only be answered in the context of identified risk.
- 2 When we talk about security, we aren't talking about objective, probabilistic events.



SECURITY METRICS MAKE SENSE ONLY IN THE CONTEXT OF RISK

- Show the maturity of your information security organization: security isn't about being compliant just at audit time but about a consistent, repeatable application and management of appropriate policies, processes, and technologies.

CEOs are often not well served by the metrics they receive. It is suggested that one reason is that because security professionals struggle with a universal understanding of what security actually is, business managers too often fall back on compliance as a measure of what they perceive as security. As a result, what the vast majority of executives expect—and what they get—is an answer that tells them how compliant they are with relevant standards. If they are compliant, they assume that they're secure. "But as important as compliance is, being compliant does not equate to being secure," says Mark.

Furthermore, some metrics conceal fundamental problems. Mark explains that we often use outdated frequentist probability models more well suited for safety engineering and financial services than the very different world of security in which we deal with adaptive threats. These models that say, "Here is the objective, quantified risk; therefore, if we spend x, y, and z, we can create this level of protection." But security isn't just about technology and expenditure.

When we see data breaches, it's not because of technology failures. Firewalls don't blow up or quit their jobs, and intrusion-detection systems don't suddenly stop working. Breaches happen when people put bad rule sets in place; bypass firewalls; forget to remove people from their Active Directory domains; deploy vulnerable apps; or do any number of other, usually predictable things that open vulnerabilities. Security is about consistent management of appropriate technology and policies. "In discussing our security posture, I would never try to answer the question of how secure are we in absolute metrical terms," says Mark. "I would say I believe that we're on the right path and here are indicators of that."

When we talk about security, we aren't talking about objective, probabilistic events. We're talking about human factors. Anything can happen. It could be that right after your security presentation to the board, your CEO says something inflammatory in a news conference, and suddenly Anonymous announces that it's going to attack your company. "Overnight, your company's risk profile fundamentally changes," says Mark.

“

In discussing our security posture ... I would say I believe that we're on the right path and here are indicators of that.

”

DEFINE SECURITY METRICS THAT ARE VALUABLE ACROSS THE C-SUITE



ANDREW STORMS

Vice President,
Security Services
New Context


Andrew Storms is the vice president of Security Services at New Context. Previously the senior director of DevOps for CloudPassage and the director of Security Operations for nCircle (acquired by Tripwire), Andrew has been leading IT, security, and compliance teams for the past two decades. His multidisciplinary background also includes product management, quality assurance, and software engineering. He is a CISSP, a member of InfraGard, and a graduate of the FBI Citizens Academy.

 |  |  |
Twitter | Website | Blog

It seems like every week a new security threat hits the Internet. From malware to phishing and distributed denial-of-service attacks, every time an organization figures out which threat is most important, a new one pops up. That leaves organizations constantly scrambling to ensure that they're protected. For chief information officers and chief information security officers, that means spending a lot of time trying to explain to members of the C suite why they must invest capital in specific security technologies and functionality.

Andrew Storms, vice president of Security Services at New Context, a DevOps consultancy, says that that's part of the challenge when it comes to creating security. "It's one of those questions," he says. "Can you ever be 100 percent secure? The question itself assumes that you could be." In most cases, says Storms, that's not the case, though. "There's a saying: the most secure system is the one that's not connected or is turned off." Yet, it's impossible to keep all your systems turned off or disconnected all the time.

"No single set of metrics works for everybody." Instead, says Storms, organizations should look at risk through the same lens they use to evaluate risk in financial markets. "Let's define the risk profile that you're willing to live with—one that you can sleep with. If we take that risk management approach, we ask similar questions to what we would in financial markets based on what you're looking to invest in."

“ We need to agree on the metrics that make the most sense to everybody across the entire C suite. ” 

KEY LESSONS

- 1 Focusing on metrics just to have metrics won't help keep an organization secure. Instead, the focus should be on metrics that are specific to the company.
- 2 Focus on metrics that you can track and improve consistently over time rather than focusing on whatever metrics happen to look good when security is questioned.

DEFINE SECURITY METRICS THAT ARE VALUABLE ACROSS THE C-SUITE

Storms says that it begins by looking at the company profile and its important assets. “Are you holding financial data or personally identifiable information on your customers? What are attackers going to go after, and what’s the worst damage they can do to your company? What are the most important things to you? Then, you build a risk analysis around those answers.”

Typically, says Storms, organizations try to pull metrics from a disparate set of tools, such as compliance tools or vendor data, and distill that information into a quantifiable system against which they can make comparisons. “There’s nothing wrong with this: you’ve defined something that you can track over time, and that’s way more important than answering the question, ‘How secure are we?’ You’ll never be 100 percent secure, but you can work over time to reduce risk and make things more secure. That’s the sauce. That’s the ‘secret sauce.’”

However, Storms believes that when you select metrics that you can track over time and improve consistently, it’s far more important to choose relevant metrics than to try to maintain multiple metrics that have little or no bearing on actual security. In addition, he doesn’t think it’s a good idea to switch among metrics just because one looks more attractive than another. In fact, some metrics become less valuable after a while, says Storms. “They’re the ones that just aren’t granular enough to provide prioritization.”

Most importantly, says Storms, everyone needs to agree which metrics are important. “We need to agree on the metrics that make the most sense to everybody across the entire C suite. It’s not just the chief executive officer: it’s the head of finance, the head of marketing, the head of human resources. Security isn’t just the job of the security person and his or her department, it’s everyone’s job, and that’s something that we constantly harp on that people don’t always think about.”

“

Security isn't just the job of the security person and his or her department, it's everyone's job.

”

SECURITY METRICS ARE ABOUT ILLUSTRATING CRITICALITY VS RISK



**GENADY
VISHNEVETSKY**
CISO
Stewart Title Guaranty
Company

Genady Vishnevetsky is the CISO for Stewart Information Services Corporation. An established leader with experience in building successful security programs to protect enterprise against emerging threats, Vishnevetsky leads the security, governance, and compliance programs for a major real estate financial services company. In his past role as the vice president of security and information security officer at Paymetric, Genady built the cybersecurity, governance, and compliance programs for the United States' fifth largest payment processor of card-not-present electronic payments systems.



Website

“Your chief executive officer (CEO) isn’t interested in how many vulnerabilities you have,” says Genady Vishnevetsky, chief information security officer of Stewart Title Guaranty Company. That’s not to say that the number of vulnerabilities isn’t important, just that when you’re communicating the strength of corporate security program to your CEO and other members of the C suite, metrics like the number of vulnerabilities won’t provide useful information.

“The reality is, your program has to be risk driven,” says Vishnevetsky. “The same vulnerability can have different impacts on the asset, based on many factors.” Thus, your priority of addressing the vulnerabilities has to be directly related to risk of the asset to business. He explains using the example that by assigning each asset a level of criticality, if security is breached on a very critical asset, even if it has fewer vulnerabilities, it can cause substantial loss of revenue, reputation and even bring the company down. Alternately, you can have assets that have hundreds of vulnerabilities, but those assets have no associated critical data. The number of vulnerabilities may appear high, but because they’re lower on a scale of criticality, the risk is lower, as well.

“ 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. ”

KEY LESSONS

- 1 Metrics are useful for gathering information about vulnerabilities, but until those metrics are distilled into something the CEO understands, they’re nothing more than numbers.
- 2 Stay away from large, raw metrics. Instead, present security and vulnerabilities as a scale of criticality versus risk.



SECURITY METRICS ARE ABOUT ILLUSTRATING CRITICALITY VS RISK

Vishnevetsky says the most effective way to determine which metrics are important is to use a computational method that determines the value of an asset or set of assets to the business, physical location of the asset, segmentation, additional compensating controls and what types of vulnerabilities exist for those assets. That allows organizations to build a solid picture of the criticality of those assets. “These compile into metrics that convert these vulnerabilities or threats into a risk factor,” says Vishnevetsky. “So, this particular asset has a risk factor: assign it a number from 1 to 5, 1 to 10, or 1 to 100—it doesn’t really matter. It’s all comparative. You show your assets according to value as opposed to looking just at the number of vulnerabilities.”

When communicating the strength of your security program to the C suite, Vishnevetsky says that it’s important not to overwhelm them. “If I’m presenting to the executive team, it depends who’s on that team. Different executives will better understand metrics that are dear to their heart. You cannot tailor your metrics to every executive,” he says, “but you can select at most five metrics that are both qualitative and quantitative, and each individual will pick up something he or she understands.”

For example, Vishnevetsky says that the CEO will understand maturity level: our security program has a maturity of three out of five in this domain. In another domain, it has a maturity of one out of five, and another domain has a maturity level of four out of five. “That’s what they understand,” he explains. “It needs to be visual. It needs to be concise. It needs to be simple. Remember, they are not technologists who understand what the vulnerability is. They understand the risk to the business, and they understand the capability of your security program as far as how well it defends the business, how it helps to protect the business. That’s what they understand.”

“The CEO probably needs to feel comfortable that you “get it,” that you know what you’re doing. You can present him or her one or two simple metrics, usually a maturity and capability level of your security program,” he adds. “One or two and no more than that. That’s about all the metrics a CEO needs to know. Anything that deals with the number of viruses, number of vulnerabilities, number of penetration testing, number of scans—any massive numbers are going to blow their minds.”

“

They are not technologists who understand what the vulnerability is. They understand the risk to the business.

”

SECURITY METRICS NEED VALIDATION AND CONTEXT



**TREVOR
HAWTHORN**

CTO
Wombat Security
Technologies

Trevor has 20 years of technical information security industry experience in both operations and consulting. His career has focused on security assessments, cloud security, and technology leadership. Prior to Wombat, he was co-founder and CTO at ThreatSim (acquired by Wombat in October 2015). Trevor has held senior positions at Stratum Security, CyberTrust, and UUNET Technologies, and he has presented to numerous commercial and government organizations worldwide.

 |  | 
Twitter | Website | Blog

There was a time when information security was something you added to the business—an extra layer of protection, like insurance—and it often received scant attention in the board room. That’s no longer the case. Today, security is baked into business operations. “Security has become a big C suite topic, both from the perspective of risk from outside attack and meeting compliance requirements,” says Trevor Hawthorn.

To work in the boardroom, metrics must quickly encapsulate the business’ security posture, and that’s not always so easy to do. “Metrics must include business context to be meaningful,” says Hawthorn.

One high-level security metric consists of three parts, which comprise ‘risk’:

- **A vulnerability metric.** This might be a combination of patch management efficacy or data derived from a vulnerability management solution or some other metric that provides an indication of the business’ exposure to exploits.
- **A threat metric.** This metric provides an indication of the likelihood that a data compromise will incur some kind of operational and remediation cost to the business. The metric might consist of different threat types, such as unauthorized access, misuse of data, and the likelihood of employees or executives being victims of phishing attacks.

“ Just looking at these vulnerability statistics is not enough. You also need to validate them and put them in context. ”



KEY LESSONS

- 1 To work in the boardroom, metrics must encapsulate the business’ security posture, and that’s not always so easy to do.
- 2 The best way to validate your security metrics is through third-party risk assessment and penetration testing.

SECURITY METRICS NEED VALIDATION AND CONTEXT

- **Asset value.** This metric includes an assessment of data types, such as intellectual property, financial data, or personal data, and estimates of their value to the organization.

Combining these three metrics in different ways gives the board a high-level view of how well protected the business is against a breach and what the cost would be in the event of a breach. Contained within these calculations are metrics that support a finer look at the security posture. For instance, you would be able to deconstruct the threat metric to determine the likeliest sources of attack, or you could drill into the vulnerability metric to discover your greatest security weaknesses. “But just looking at these vulnerability statistics is not enough,” explains Hawthorn. “You also need to validate them and put them in context.”

Hawthorn says, “Validating high-level security metrics is important because they are only statistics: you need to prove they mean something.” So, how do you validate your security posture metrics? The best way is through third-party risk assessment and penetration testing. Ideally, third-party vendors would conduct such testing at different times, because you’re looking for objective consistency in the results. “You want the testing to support your own metrics, but if it doesn’t, you have a basis for taking another look at what you’re doing,” says Hawthorn.

Still, the business needs operational context for all these metrics. One way a business can put its metrics in context is to compare them against risk frameworks, which provide guidelines about how to assess security risks and preparedness. Several frameworks exist, many of them industry specific. It’s not exact, but as Hawthorn says, “The value of this comparison is that it gives a general idea of how good or bad a company’s security posture is compared to others in an industry segment.”

Armed with security posture metrics derived from your own systems, third-party assessments that validate those metrics, and industry frameworks that offer a general idea of how you stand in your industry, you have the basis for a conversation with executives that focuses on building a secure business strategy.

“

You want testing to support your own metrics, but if it doesn't, you have a basis for taking another look at what you're doing.

”

PRESENT SECURITY METRICS USING RISK-BASED LANGUAGE



**SCOTT
SINGER**

CISO
PaR Systems, Inc.

Scott Singer is the CSIO for PaR Systems, an industrial automation company. Before PaR, Scott spent 16 years with Medtronic in various leadership positions, including as the European infrastructure manager and a division CIO. In his last two years at Medtronic, Scott led the global security function. As a Naval Reservist, Captain Singer is the Navy Emergency Preparedness Liaison Officer (NEPLO) for the state of MN. Prior to be promoted to NEPLO, he was executive officer of a Pacific Fleet cyber-security unit.

  
Twitter | Website | Blog


In chief executive officer (CEO)- and board-level presentations, you must use security metrics carefully. “If I start using technical security terms and metrics, I completely lose the audience,” says Scott Singer, who wears both the chief information officer and chief information security officer hats at PaR Systems, a company that develops industrial automation systems.

At the same time, you can't come across as arbitrary. You must be able to support the proposals you're making and the positions you're taking. Singer says, “It's important to raise issues using a risk-based language that allows the board to make risk-based decisions on cyber-security spending.”

In many cases, board and CEO presentations focus on particular issues they must address or decisions they need to make. Singer cites an example of a presentation he gave to the board after the company was breached. He had to explain what happened and propose a solution that would help them to avoid that problem in the future. Par Systems is a technology company, and it has a strong board. Many of its members have some familiarity with cyber-security. Even so, the members would be looking at the problem from a business perspective, not just from a technical perspective. Singer's approach was to begin with a subset of board members who had a strong technical background and present to them first. “I made a small, ad hoc cyber-security subcommittee of board members, used them as a sounding board for input, then went to the full board meeting with my presentation.”

KEY LESSONS

- 1 In many cases, board and CEO presentations focus on particular issues they must address or decisions they need to make.
- 2 To make a decision, the board needs security information in the context of risk, risk mitigation, and costs associated with eliminating that kind of threat.

“ If I start using technical security terms and metrics, I completely lose the audience. ” 

PRESENT SECURITY METRICS USING RISK-BASED LANGUAGE

In this case, Singer relied on metrics that were relevant to the breach in question. One set of metrics related to an advanced persistent threat (APT) attack. They included information about how long an attacker was in the system before he or she began stealing data and how long it took to detect the breach. Just presenting those numbers wouldn't help to the board make a decision, however, so Singer had to present the data in the context of risk, risk mitigation, and costs associated with eliminating that kind of threat.

The goal from a security management perspective was to reduce the time between when an attacker first enters the system and when that attacker is neutralized from 200 days, which is where the company was, to 2 days. To achieve that goal, Singer presented options to the board, each with its associated costs.

"I gave them choices," explains Singer. "Based on some metrics, I could offer them three levels of protection and their associated costs." Each option was also related to ongoing levels of risk so that the board could make their risk appetite judgment in the context of the costs of risk mitigation at those levels of protection. Rather than going into technical details about each proposed solution, Singer kept it simple, describing the solutions in terms of closing doors to potential attackers. At this point, the board was not interested in the technical details.

The presentation went well, and he got approval for what he needed to narrow that particular attack window. The "days of vulnerability" metric associated with APT attacks became a simple way of showing the progress his organization was making toward achieving the goal of getting to two days. "I use that as a metric to see how well we're doing," says Singer.

“

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

”

SECURITY METRICS: IT'S A COMPOSITE IMAGE



**ROY
MELLINGER**

VP, IT Security, and CISO
Anthem, Inc.

Roy Mellinger is vice president of Information Technology Security and CISO at Anthem, overseeing a department of over 300 information security and risk management professionals. Prior to joining Anthem, he served in executive security leadership positions for Sallie Mae, GE Capital, Heller Financial, Household International, Inc. and Spiegel. Mr. Mellinger is a CISSP, with advanced certifications in Security Architecture and Information Security Management. He is on the Board of Directors for HITRUST, and the Advisory Board for The Lares Institute.

As a chief information security officer (CISO), you can't control what you don't understand, Anthem CISO Roy Mellinger affirms. "You can't manage what you don't measure," he adds. "And you can't measure what you don't monitor."

There is, however, an extra step to take before your metrics monitoring can even begin: you must take a step back and decide the information security priorities for your organization, Mellinger asserts. "You have to decide which metrics are strategically aligned with your security roadmap," he says. At Anthem, Mellinger tends to communicate high-level metrics to senior leaders who want to know where the business stands on information security. In effect, his three recommendations are composite bundles that encompass a wide variety of submetrics:

- **Risk posture.** He defines this as a measurement that gauges overall information security risk. "That is going to be your patch-management life cycle, what kind of network-probing intrusions you're seeing, and whether you're experiencing any breaches or failures," he says. Depending on your company and industry vertical, this category could include from four to a dozen metrics or more. "To me, it's a composite score," Mellinger says. "Overall, what does our risk posture look like from a network security perspective? From a risk management perspective? Where are we?"

“ You have to decide which metrics are strategically aligned with your security roadmap. ”



KEY LESSONS

- 1 Before your metrics monitoring can even begin, you must first decide the IT security priorities for your organization.
- 2 The information security metrics that senior leaders tend to cherish most are those that show them how their business stacks up against their competitors.

SECURITY METRICS: IT'S A COMPOSITE IMAGE

- **Sensitive data exposure.** Mellinger advocates defining sensitive data according to your organization's priorities. The category could include electronic protected health information, personally identifiable information, or intellectual property. Many metrics factor in when monitoring for data exposure, he says. "Are we encrypting everything? Do we have projects to encrypt? Have we had misuse or abuse? Have we had data leakage? Have we had human error?"
- **Alignment with competitors.** At first blush, this might not sound like a metric at all. In fact, Mellinger says, it's the metric executives ask him for most. To Mellinger, it describes the state of organizational governance. What are the internal and external audit gaps? Are they being closed? Is the organization green on the heat map (in good shape), amber (average), or red (poor)? Anthem often brings in professional audit firm Ernst & Young to rate how Anthem is succeeding at host, security, and third-party management among other metrics. The results are compiled into a spider graph for presentation to leadership. Anthem's various ratings can be overlaid with the composite score of other companies in the vertical, Mellinger says, letting executives know how their efforts compare to those of their competitors, Mellinger adds. He often invites auditors from PricewaterhouseCoopers in afterward to validate Ernst & Young's results. Executives love leading their peers when it comes to information security and never want to fall behind, but, Mellinger concedes, "They often don't mind if they are in the middle of the pack."

“

You can't give senior leaders tons of metrics. You need to boil that information down to a high-level, C suite–type discussion.

”



SECURITY METRICS: IT'S A COMPOSITE IMAGE

He offers another piece of advice for the young CISO. "I learned a long time ago that you always answer in threes," he says. He advocates three-point presentations that follow this pattern:

- Refresh senior leaders on what you spoke about during your last meeting.
- Update them on the progress you have made on their previous requests.
- Describe the key issues on which you're focused at present in addition to any emerging issues that you think executives need to know. "Share everything," he adds, "but not from a the-sky-is-falling perspective. I don't think that ever works."

No metrics should be off the table in those meetings, but, he adds, "You can't give senior leaders tons of metrics. You need to boil that information down to a high-level, C suite-type discussion." If the CIO, chief executive officer or a board member wants a deeper dive, feel free to schedule a private meeting and speak in-depth about your metrics, Mellinger urges. "The more executives know," he emphasizes, "the more supportive they are."

“

The more executives know, the more supportive they are.

”



Do you really know your **risk profile?**

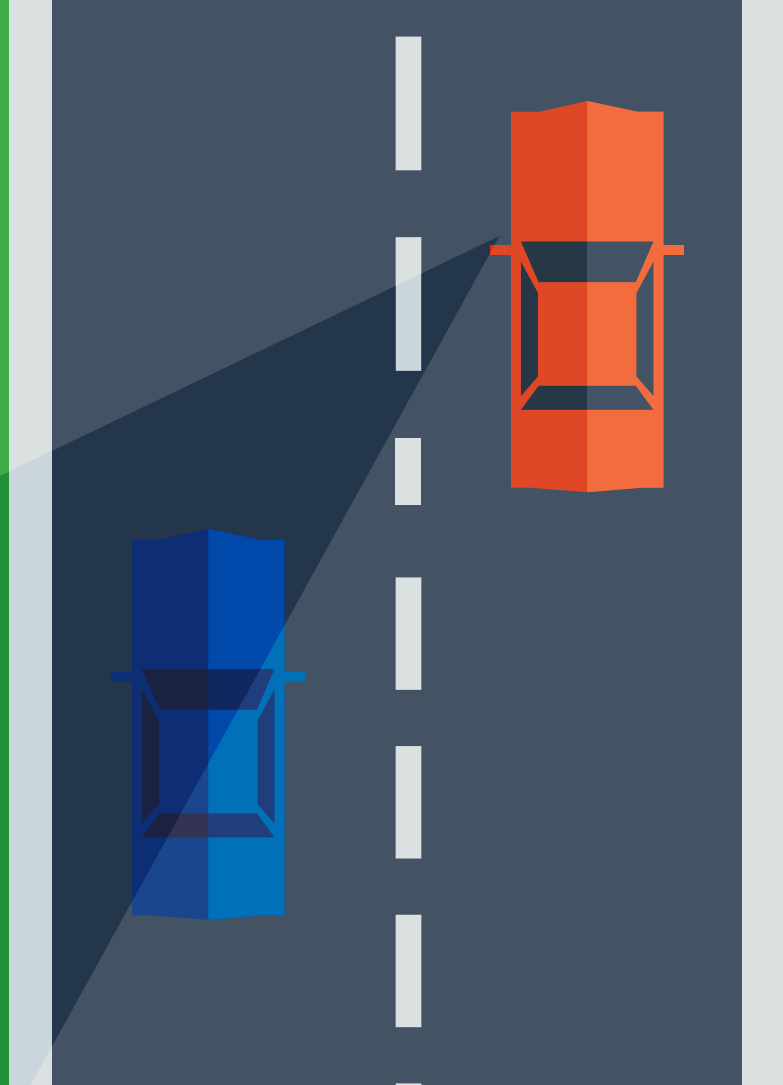
Mobile employees, transient devices, cloud applications, and other new technologies all introduce new - and often unknown - levels of risk.



Download Now
Free Whitepaper

Read *Eliminating
Cybersecurity Blind Spots.*

Reduce unknown and unmanaged risk.



Security Metrics for Threat Management

In this Section...



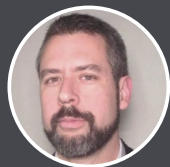
Aanchal Gupta
Microsoft.....55



Julian Waits
PivotPoint Risk Analytics.....62



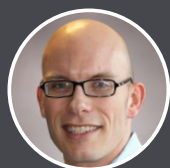
Jonathan Chow
Live Nation Entertainment.....57



Wolfgang Goerlich
Creative Breakthroughs Inc.....65



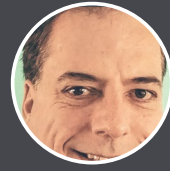
Vikas Bhatia
Kalki Consulting.....60



Dave Shackelford
Voodoo Security.....68



Ed Adams
Security Innovation, Inc.....70



Steven Parker
The Advisory Board
Company.....74



Roota Almeida
Delta Dental of New Jersey.....72

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 | Blog



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?’”

“

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

”

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.”

WITH SECURITY METRICS, YOU DON'T HAVE TO SWEAT THE DETAILS



**JONATHAN
CHOW**

Senior VP, CISO
Live Nation Entertainment

Jonathan Chow is senior VP and CISO for Live Nation Entertainment, where he is responsible for the implementation and monitoring of the enterprise-wide information Security program. He is a popular speaker and has received several awards, including the Premier 100 IT Leaders by *Computerworld*, the Information Security Executive of the Year People's Choice Award from the T.E.N. Executive Leadership Program, and Global CISO Top 10 Breakaway Leaders by Evanta.



It was only a few years ago, as he was taking his current job as chief information security officer and senior vice president at Live Nation Entertainment, that Jonathan Chow discovered how important it is to focus on metrics that really matter to the business. His task at the time was to build a security program from scratch. "When we first started to get the numbers, they were pretty abysmal," Chow states. Nobody had asked the security team to measure security metrics before. "Quite honestly," he recalls, "it was overwhelming."

Chow's answer was to shift his team's thinking on security. "We started to make it higher level. We weren't focusing so much on specific vulnerabilities," he comments. Instead, he focused on three macro-level metrics:

- **Average vulnerabilities per end point.** You naturally want to know the relative vulnerability of your enterprise computers, company-issued mobile phones and tablets, and other end-user systems, Chow says, but unless you put that into context, you could easily get a skewed view. Measuring in terms of average per device is a great way to get a grip on the relative security of the enterprise, Chow says. You might find your average vulnerability per system was 24 last year, and this year it's down to two, for instance. "That is a metric I would bring up to the chief executive officer and to the board," he says.

“ We started to make it higher level. We weren't focusing so much on specific vulnerabilities. ”

KEY LESSONS

- 1 Tracking metrics in terms of averages rather than raw vulnerability counts is a great way to keep security improvements in perspective.
- 2 Becoming totally secure is an elusive if not impossible goal. The real point is to show continuous evolution and improvement.



WITH SECURITY METRICS, YOU DON'T HAVE TO SWEAT THE DETAILS

- **Average vulnerabilities per application.** This tells a similar story to the previous metric, but Chow thinks that it's important to measure software vulnerabilities separately from end point vulnerabilities. "People write software, and so there are vulnerabilities in the software," he states. Just as in the case of end point vulnerabilities, this metric is about tracking trends, he remarks. "If you keep driving that average down," he says, "it gives you more confidence."
- **Average time to patch.** Patching is a baseline security measurement for Chow. Again, he measures the time in terms averages rather than tabulating a raw missing-patch count. "I don't look at this metric as though this system is missing 3 patches, this one is missing 15, while this one is perfect," he says. Monitoring average patch time offers him a barometer by which to gauge how well his organization is functioning, he states. "I don't necessarily care that this one machine is missing 1,000 patches," he contends. "If everything else is fine, that shows me that the operation itself generally is doing well."

Nothing will ever be perfect, Chow acknowledges, but these metrics help reveal whether the organization is struggling. One example of a metric that he thinks would not help as much is monitoring the number of company devices that are lost or stolen. He used to do that but stopped. Clearly, it's an important issue: when someone loses a laptop containing last year's budget, you have a problem, but there's nothing the security team can do to fix it beyond talking to people and asking them to be more careful, he says.

The focal shift that led Chow to approach security metrics differently gave him a new approach to communicating about security with executives. By addressing these issues holistically rather than obsessing over details, he found he could communicate with leadership at their level. They want to hear a story, he says, and they want it backed up with facts.

“

If you keep driving that average down, it gives you more confidence.

”



WITH SECURITY METRICS, YOU DON'T HAVE TO SWEAT THE DETAILS

“When I go to the board, I bring data,” Chow comments. “Because data are not emotional. The data either give me more confidence that we’re becoming more secure or make me worry that we’re not improving.”

In the end, he says, the point is not to convince executives that you’re completely secure—that’s an elusive if not an impossible goal, he believes—but rather to demonstrate that you’re continually evolving and improving information security. “I say, here is our performance, here is how we’re trending: we’re getting better every quarter,” Chow says. “I point to the data.”

“

Data are not emotional. The data either give me more confidence that we’re becoming more secure or make me worry that we’re not improving.

”

THE KEY: LINKING SECURITY METRICS TO BUSINESS OBJECTIVES



**VIKAS
BHATIA**

CEO & Founder
Kalki Consulting

Vikas Bhatia is the founder, CEO, and executive risk adviser at Kalki Consulting. With more than 15 years of experience serving local, regional, and global clients in the outsourcing, consulting, and regulatory domains, he can enhance any organization's information security management system. Vikas is a Certified Chief Information Security Officer, Certified Information Systems Security Professional, and Certified Information Privacy Professional.



Twitter | Website | Blog



“The first thing the chief executive officer (CEO) or board wants is to be aware that a risk exists,” says Vikas Bhatia. The CEO is looking at the chief information security officer (CISO) and his or her organization to adequately assess the risk and prioritize it. The CEO needs to know how important the risk is. “Many technical CISOs are unable to quantify the impact of a risk to the business,” says Bhatia, “and this is often the source of confusion around appropriate security strategy.”

It all begins with how you view and measure threats to your data. “Most security organizations still perceive the security problem as an outside-in problem, but we view it as having three parts,” explains Bhatia:

- **External threats.** One-third of the threat is external: outsiders trying to get into the network. These outsiders could be malicious hackers, disgruntled former employees, threat nations, and the like.
- **Internal threats.** One-third of the threat consists of attacks initiated by internal “trusted resources.”
- **Technical misconfigurations or coverage gaps.** The remaining third is initiated by technical resources that either intentionally or unintentionally leave some kind of vulnerability or gap in the environment that then results in an attack or breach.

“ Many technical CISOs are unable to quantify the impact of a risk to the business. ”

KEY LESSONS

- 1 The CEO is looking to the CISO and the CISO's organization to adequately assess the risk and prioritize it.
- 2 Rather than reporting on the ROI for one piece of equipment, it's best to present the board with information showing how the investment has affected the business' overall security posture over time.



THE KEY: LINKING SECURITY METRICS TO BUSINESS OBJECTIVES

Bhatia says, “Metrics are tied to each of those components, and you must look at them together rather than individually.” Then, for the CEO’s benefit, the CISO must be able to show the significance of those metrics to the business. For example, if you tell the executive team that you need a firewall, what does that really mean to the business? If the CISO is able to present the risks and quantify them in terms of their impact on the business, then the business can more effectively manage its risk.

Too often, a budget allocation by the board results in a request to show the return on investment ROI for one piece of equipment. The CISO and security team then scramble to show ROI, because that’s how they must demonstrate the value of this expenditure. But as Bhatia explains the problem, “What they really need is a presentation showing how the expenditure fits with the overall posture as it relates to each of the three threat components, and then trending metrics for those components over time.”

For instance, if you buy a piece of perimeter equipment to address known external threats, you can show the number of attacks or successful penetrations trending down after the implementation of this new equipment. If at the same time, however, you can show a decline in an internal risk—for example, the number of employee attempts at unauthorized access of pay chart data, both successful and unsuccessful—and you can attribute favorable trends in those metrics to the new equipment, you’re proving that the new technology is delivering greater value by mitigating risk in another part of the overall security posture. “Now you’re demonstrating a better-than-expected ROI on that security investment,” says Bhatia.

There have been big changes in IT infrastructure, technology, and the way risk metrics are collected, but the overall method and the approach that experienced CISOs apply to risk haven’t changed much. “If an organization has a rich management framework that aligns with its business objectives,” says Bhatia, “and if it uses metrics that show board members and executives the value of security initiatives in meeting business goals, then it doesn’t matter whether the technology is in the cloud, on premises, up the stack, down the stack, remote, wearable, Internet of Things, or anywhere.” It’s still the same fundamental approach to assessing risks and justifying security priorities.

“

Metrics are tied to each of those three components, and you must look at them together rather than individually.

”



**JULIAN
WAITS**

CEO
PivotPoint Risk Analytics

Julian Waits is CEO of PivotPoint Risk Analytics and has more than 20 years of experience in the IT and security markets. Prior to joining PivotPoint, Julian served as the CEO of several companies, including ThreatTrack Security, Brabeion Software, IT GRC Software, and Way2Market360 and held senior leadership positions at Archer Technologies, e-Security, and BNX Systems. He is an alumnus of Loyola University New Orleans and Xavier University.



When a chief executive officer (CEO) asks the question, “Just how secure are we?” Julian Waits thinks that the chief information security officer (CISO) should be prepared to answer with metrics on the applications, processes, and end users that matter most. “Whatever metrics you’re going to share with the CEO, board, or executives, you need to prioritize them around the things that are most important to the business,” Waits states.

Speaking as a CEO who has worked as an IT Security Manager in the past, Waits identifies three key metrics that he thinks CISOs should always monitor:

- **Patch rates.** Time to deploy or update mission-critical applications and operating systems in devices that are attached to the network is a key metric, Waits asserts. Using technologies like Tenable SecurityCenter, he says, you can measure this time easily. “As the environment changes, as you add new applications to the environment, you should be continuously monitoring updates,” he suggests.

“ Whatever metrics you're going to share with the CEO, board, or executives, you need to prioritize them around the things that are most important to the business. ”

KEY LESSONS

- 1 The CISO should be prepared to answer a CEO's questions using metrics on the applications, processes, and end users that matter most.
- 2 The CISO must play educator to the CEO as well as the other key end users. Metrics are an important way to ensure that the word is getting out.



USING SECURITY METRICS TO DEFEND THE BUSINESS

Focus your greatest efforts on keeping track of systems that keep the business functioning, he advises. Don't try to track every single application or device upgrade throughout the enterprise. "I don't think anybody can manage everything effectively," he says, adding that statistics are proving that. "The breach rates are increasing astronomically," he says.

- **Infrastructure updates.** This metric is about monitoring updates to systems inside the network—routers, next-generation gateway interfaces, firewalls, etc.—rather than devices and software systems that are attached to the network. Waits says that he's stunned by how often he has visited companies that conscientiously monitor business application patches and operating system updates but don't know when they last upgraded their interior firewall software. "That's not solving the whole problem," he states.
- **The human metric.** People are easily the top compromise vector, Waits says. The easiest way to exploit their weakness is through email phishing attacks. It may seem counterintuitive to list people as a metric, but Waits notes that you can statistically measure end users' phishing awareness. Tools are commercially available that allow companies to stage intentional, nonmalignant phishing attacks through email on their own end users and measure the outcomes. Are employees recognizing and responding appropriately to these vulnerabilities? Staged attacks are only done in Waits' company after employees have completed phishing awareness training, so these tests can help determine whether employees are learning to spot and reject malicious email.

"All of this should start with educating your end users," Waits says. That, he notes from personal experience, will probably include the CEO.

“

These phishing attacks are becoming very sophisticated. It's not about careless end users anymore; it's just that this stuff is good.

”



USING SECURITY METRICS TO DEFEND THE BUSINESS

When Waits was CEO at a previous company, he was successfully phished, despite the fact that he was a security expert in his own right. It started with a strange email from his bank. It contained an unsecured PDF attachment that accurately listed the company's recent transactions. He and his bank had previously agreed that such information would not be shared in unsecured formats, so he angrily called his bank to complain. That's when he realized he'd been had.

The bank had not sent the suspicious email; it had not even sent out monthly statements. Despite the accuracy of the PDF's transaction record, the email was a fraud, laced with malware. Eventually the Federal Bureau of Investigation caught the perpetrators, but Waits still doesn't know how they obtained his company's transaction record.

"I used to use the term *careless end users*," Waits recalls. "Then, I realized that these phishing attacks are becoming very sophisticated. It's not about careless end users anymore; it's just that this stuff is good."

He concludes that the CISO must not only communicate security risks in a business language that the CEO can understand but must also protect the CEO from him- or herself in instances like the one Waits fell prey to. In other words, the CISO must play educator to the CEO as well as all other key end users. Metrics are an important way to ensure that the word is getting out.

"The CISO is, in many senses, the defender of the business' ability to perform its function," Waits says. "Therefore, education—focusing on the fundamentals and, most importantly, understanding what components they are securing that are most important to the business—is everything."

“

The CISO is, in many senses, the defender of the business' ability to perform its function.

”



J. WOLFGANG GOERLICH

Director of Security Strategy
CBI
(Creative Breakthroughs Inc.)

J. Wolfgang Goerlich is a director of security strategy with CBI. Prior to joining CBI, Wolfgang held roles such as vice president of consulting and security officer. He co-founded OWASP Detroit, organizes the annual Converge and BSides Detroit conferences, and is an active member of the security community, regularly presenting at conferences on topics such as risk management, incident response, business continuity, and secure development life cycles.

  
Twitter | Website | Blog

To determine whether your company is secure, J. Wolfgang Goerlich believes that you must take a pragmatic look at your controls and the real threats you face. Goerlich stresses that quality intelligence is necessary to conduct that assessment. “You must obtain good intelligence as to your internal state, what’s happening across the industry, and which threats are directed at you,” he explains.

When evaluating your internal state, Goerlich recommends considering security metrics, such as the types of attacks you’re seeing at the moment and where they are originating, and assessing the type of projects your staff are working on that might encourage those types of attacks. You can find these metrics by tapping your systems for internal intrusion detection and prevention, data loss prevention, vulnerability management, and security information management. With your internal metrics in place, use them to spot trends that indicate what types of attacks are commonly happening internally. Map those trends, threat-model them, then outline your detective and preventative controls for those kinds of attacks.

“ You must obtain good intelligence as to your internal state, what's happening across the industry, and which threats are directed at you. ”

KEY LESSONS

- 1 To determine the best security metrics for your organization, gather quality intelligence on the internal and external threats unique to your environment.
- 2 When communicating your company’s security posture to the CEO, use specific examples that are supported by data and actionable.



Next, it's time to look at external attacks. You can also use the latter half of the process for analyzing internal attacks—threat modeling, prevention detection, and frequency and impact analysis—to look at external attacks. This is where threat intelligence becomes a factor: you can consider what types of attacks are happening to your peers, what types of attacks are happening across the Internet, and what types of attack factors are commonly occurring.

There are several sources for this kind of threat intelligence. For example, each industry has information sharing and analysis centers (ISACs). "An ISAC allows you to share information under the guise of nondisclosure, and that information is protected, so you can share more of it. You can share what types of attacks you're actually seeing right now," says Goerlich. Government-sponsored initiatives exist, as well, to foster information sharing.

Unofficial channels are also a valuable source of threat intelligence. Explains Goerlich, "This type of threat intelligence is often shared at a bar over drinks or at your local coffee shop over a mocha. It happens when you sit down with your peers and say, 'Hey, what are you seeing?'" The threat intelligence insight shared in such conversations can be especially useful because it's not the kind of information that's publicly disclosed or accessible by other means.

When you have acquired this external threat intelligence, the next steps are to perform a threat model on it, look at how the attacker would execute that attack, then consider how likely it is to take place and what the impact would be. Such an attack might be one that your organization hasn't encountered yet but your peers have, an attack that's in the news, or a threat that experts considered likely to target your type of organization. You can create a metric that explains how often or what percentage of the time you can prevent and detect this type of attack.

“

An ISAC allows you to share information under the guise of nondisclosure, and that information is protected, so you can share more of it.

”



STRENGTHEN SECURITY BY GATHERING QUALITY THREAT INTELLIGENCE METRICS

With your internal and external threats defined and assessed, give careful thought to how you will present information on your company's security posture to the chief executive officer. Advises Goerlich, "You should have specific, tangible examples that are backed up with data and that have a clear outcome."

Best practices, although sometimes helpful when considering which specific measures are useful for your company, should not be the sole factor in determining the steps you take to address your unique threats. Rather, by conducting careful assessments to understand the key internal and external threats that make up your security landscape, you can take informed action to defend your environment against the attacks that are most likely to have the greatest impact on your firm.

“

You should have specific, tangible examples that are backed up with data and that have a clear outcome.

”

MAKE SECURITY METRICS YOUR CHAOS INDICATOR



DAVE SHACKLEFORD
CEO
Voodoo Security

Dave Shackelford is CEO and principal consultant at Voodoo Security, lead faculty at IANS, and a SANS senior instructor and course author. He has consulted with hundreds of organizations in the areas of security, compliance, and network architecture and engineering. Dave is the author of the Sybex book *Virtualization Security: Protecting Virtualized Environments*, currently serves on the board of directors at the SANS Technology Institute, and helps lead the Atlanta chapter of the Cloud Security Alliance.

  
Twitter | Website | Blog

Business is a language of measurable numbers—metrics. Any competent chief information security officer (CISO) can offer up metrics that help shape the C suite’s understanding of IT security and score resources needed to protect the environment, says consultant and industry influencer Dave Shackelford. But select them with purpose.

“If you tell business people, ‘Hey, look at all these systems that have antivirus!’ Who cares?’ he says ruefully. “What does that even mean to me?”

Instead, Shackelford recommends monitoring the following metrics, each of which is a key chaos indicator:

- **Unapproved configuration changes.** Such changes include unauthorized services, user IDs, and software installations on the network. Tracking the frequency of such events tells you whether users are following internal policies. They can also be your best shot at detecting breaches. It’s how Shackelford once uncovered a stash of millions of credit card numbers on a client’s network—numbers that did not belong to his client’s customers but had been deposited by thieves who stole them from another business.

“If you tell business people, ‘Hey, look at all these systems that have antivirus!’ Who cares? What does that even mean to me?”

KEY LESSONS

- 1 Choose metrics purposefully. Tracking unapproved configuration changes makes sense; tracking the number of antivirus installations probably doesn’t.
- 2 CISOs should constantly chart their IT environment and keep tracked metrics close at hand, to be communicated at a moment’s notice.



MAKE SECURITY METRICS YOUR CHAOS INDICATOR

The client company never noticed they were there. Shackleford's client was not sued, but its officers had to give depositions and courtroom evidence. "It was a big, messy ordeal," Shackleford says. "If they had been paying attention, they may have had a much better chance of avoiding the issue."

- **Missed patches.** Shackleford says it boggles his mind how often he gains access to corporate networks through missing patches—patches about which software vendors routinely issue alerts. If an enterprise consistently fails to implement high-severity patches, it indicates deep systemic problems, he warns. "Either you don't have enough people or enough time to test or you have apathy," Shackleford contends. "Something is preventing an incredibly critical operation from occurring." It's a problem that calls for immediate investigation, he says. After all, even if the CISO is not actually at fault, you can bet that he or she will be held accountable. "The CISO," he says, "is really number one in the hot seat."
- **Bad behavior.** Part of Shackleford's role is penetration testing. "If you allow me to send phishing emails to your users, I will break into your network," Shackleford states flatly. He has had equally good success using phony phone calls and depositing infected USB drives in corporate lobbies to see if employees plug them into the network. It's relatively easy to monitor and track the trends of these policy violations. "A bad-behavior metric is meaningful for business executives," Shackleford offers. "They want to know whether people are doing what they're not supposed to be doing." He suggests that the CISO conduct penetration tests cyclically to determine whether education and remediation are having any effect.

CISOs should constantly chart their IT environment, Shackleford advises. Keep the results of your metrics close at hand to be communicated at a moment's notice. In this way, you gain credibility and foster communications with the C suite, who will begin to take your improvement initiatives seriously. Metrics, Shackleford says, are a means to that end. "They support the message," he concludes.

“

A bad-behavior metric is meaningful for business executives. They want to know whether people are doing what they're not supposed to be doing.

”

GOVERNMENT AGENCIES RELY TOO HEAVILY ON COMPLIANCE



**ED
ADAMS**

CEO

Security Innovation, Inc.

Ed Adams is a software executive with leadership experience in the IT security and software quality industries. He is CEO of Security Innovation. He has held senior management positions at Rational Software, Lionbridge, and MathSoft and has presented at numerous industry conferences. He is a frequently used expert for television and print media. Ed earned degrees in mechanical engineering and English literature at the University of Massachusetts prior to receiving an MBA with honors from Boston College.



Twitter | Website | Blog



When evaluating any organization's security posture at a high level, Ed Adams collects information and metrics that answer three key questions:

- **How well patched are your systems?** "The reason I start with that one metric," Adams says, "is because about 80 percent of all successful attacks take advantage of known security vulnerabilities." By pursuing a rigorous patching policy that keeps software up-to-date and patched across all systems and devices, including mobile devices, you can exponentially reduce your attack profile and block 80 percent of potentially successful attacks right out of the gate. This metric is typically a combination of metrics that might break down across systems, such as percentage of all routers that are up-to-date, percentage of all Windows Server instances, percentage of all Linux servers, percentage of all iOS devices, and so on. "I would determine the patch and update status of all of the systems. It's not a trivial task, but it's an important one," says Adams.

“Most of the government standards contain good ideas, but they are woefully insufficient for creating a sustainable security posture.”

KEY LESSONS

- 1 **Software is now running our world. If we don't create and deploy secure software, we are creating massive attack surfaces for ourselves.**
- 2 **Most government agencies are not driven by a need to achieve a certain security posture. Rather, they're driven by mandates to be compliant with security standards.**



GOVERNMENT AGENCIES RELY TOO HEAVILY ON COMPLIANCE

- **Do you filter all email that originates from email servers that are less than two days old?** This is an important one because of the growing use of phishing and highly targeted spear phishing attacks. Even with effective employee education, including executives who are increasingly the targets of these attacks, people fall for them because the ploys they use are becoming so sophisticated. The vast majority of these attacks, however, originate from mail servers that have existed for two days or less. Attackers spin up a spam server in a public cloud, conduct carpet bombing attacks, then quickly take the mail server offline. Malicious websites that infect victims of these attacks may exist for much longer, but the mail servers are short lived. Adams says, "Filtering out all email from servers that are less than two days old will eliminate a large percentage of phishing attacks."
- **What percentage of your software engineers have gone through security training and received an acceptable assessment score?** "The reason that I focus on software security," explains Adams, "is because software is now running our world. If we don't create and deploy secure software, we are creating massive attack surfaces for ourselves." A relevant metric might be percentage of engineers who meet this standard.

These metrics are equally relevant for businesses, government agencies, and nonprofit organizations. The challenge for most government agencies, except for defense and intelligence agencies whose missions include the security of their systems, is that they are not driven by a need to achieve a certain security posture. Rather, they're driven by requirements to be compliant with certain mandated standards such as the Federal Information Security Modernization Act (FISMA). "Most of the government standards like FISMA and best practices published by the National Institute of Standards and Technology contain good ideas, but they are woefully insufficient for creating a sustainable security posture," says Adams.

To further undermine the situation, if a government agency fails a compliance audit, the agency is typically given 12 to 24 months to fix the problems. This is a long time to be living with and working on systems that have known security issues. So, an additional problem with government security is that compliance is the driver. This is the tail wagging the dog. "If you put a robust security program in place, you can achieve compliance along the way, but it doesn't work in reverse," says Adams.



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



SECURITY METRICS MUST DEMONSTRATE EFFECTIVE SECURITY GOVERNANCE



**ROOTA
ALMEIDA**

Head of Information Security
Delta Dental of New Jersey

Roota Almeida is a senior IT executive and CISO responsible for the successful implementation of information security, risk and compliance systems, and strategies across multiple global industries. Currently, she is the head of information security at Delta Dental of New Jersey, responsible for managing the development and implementation of enterprise-wide information security strategy, policies, risk assessments, and controls. Roota is a recognized thought leader in the industry as well as a frequent speaker at IT summits. She has authored various articles and has interviews and podcasts to her credit.



Twitter

As Roota Almeida points out, “In today’s world, no one can assure 100 percent security.” The issue is not whether your organization will be breached but when it will be breached and how you respond. In the past, security teams heavily focused on preventing penetration into systems that contained sensitive data. Although that continues to be important, today more emphasis is placed on better detection and mitigation. “After they get in, how quickly we can detect them and mitigate the damage are what really matter,” explains Almeida.

In managing the effectiveness of detection and mitigation, Almeida looks at three key sets of metrics that must be examined together:

- **Metrics and trends that show what kinds of malicious content the system is blocking.** “If you detect an upward trend in a particular kind of attack, you can apply analytics to get a better sense of what’s happening, whether it’s something new or related to other attacks you’re experiencing,” says Almeida.
- **Metrics and trends that show how much malicious content is not getting blocked.** This is malicious content that slips through, creating incidents that require resolution. These are not necessarily big incidents, but they include everything that’s not being blocked.

“When making a security presentation, it’s important to tie security initiatives to the CEO’s initiatives and the organization’s overall goals.”

KEY LESSONS

- 1 The executive committee is interested in the anticipated outcomes of resource allocations.
- 2 There are instances where security teams deal in qualitative evaluation, but remember that the executive committee wants quantifiable answers based on quantitative metrics.



SECURITY METRICS MUST DEMONSTRATE EFFECTIVE SECURITY GOVERNANCE

- **Metrics and trends on time between detection and resolution.** This is important in evaluating risk associated with open vulnerabilities.

These are valuable metrics in ongoing threat management, but they aren't necessarily the metrics that interest chief executive officers (CEOs) and executive boards. Almeida says, "When making a security presentation to the executive committee, it's important to tie security initiatives to the CEO's initiatives and the organization's overall goals. For example, if our goal as an organization is to expand business and win more clients, I will use the security protocols we have in place to protect our onsite data to show our advantage over our competitors." It's important to change the CEO's perception of security being a cost center to realizing that improved security helps generate revenue.

The executive committee is also interested in the anticipated outcomes of resource allocations. If it is decided that an improvement is necessary in a particular area, the chief information security officer (CISO) can put together a case for that, but it can't just be a technical argument. As Almeida explains, "The CISO's challenge is to create accurate metrics for the effectiveness of governance, such as policy implementation and other, more qualitative aspects of the security program." Executives like quantitative metrics, and yet there are many instances where security teams deal in qualitative evaluation. For example, if as part of a risk-mitigation strategy you initiate a staff training program that teaches people to contact tech support whenever they see a certain kind of suspicious social media activity, you can show a quantitative metric that demonstrates which percentage of employees has received that training. The more qualitative evaluation, however, is whether the training actually changed people's behavior. You can try to figure that out by measuring a change in the volume of those kinds of calls to tech support, but is that change in call volume an indicator of successful training, or does it reflect an increase in those kinds of attacks? Executives want a quantifiable answer.

"To be successful with the executive committee, the CISO must rely on quantitative metrics that provide a clear picture of the nature of the risk and the business value of resource allocations to address it," says Almeida.

“

The CISO's challenge is to create accurate metrics for the effectiveness of governance, such as policy implementation and other, more qualitative aspects of the security program.

”

SECURITY METRICS: THE MORE YOU KNOW, THE MORE YOU GROW



**STEVEN
PARKER**

Senior Director,
Information Security
The Advisory Board Company

Steven Parker has more than 20 years of experience implementing information security programs from a risk-based perspective. He has served in executive and senior management positions, with responsibilities ranging from strategy development and execution to strategy and tactical alignment, risk management, and crisis management. Steve's certifications include CISSP, C|CISO Certified Chief Information Security Officer, CISA, CFE, and ITILv3. He is currently the senior director for information security at The Advisory Board Company.



Website | Blog

Before joining The Advisory Board Company last year, Steven Parker was the top information security officer at Arise Virtual Solutions. As a contact call center, Arise does everything from providing technical support to opening consumer loan applications. As such, it collects and guards a great deal of personal information.

“Very often, we would have quarterly updates around our security posture,” Parker recalls. “And the question from the chief executive officer was always, ‘How secure are we?’”

Parker's security framework supplied part of that answer. He based Arise's security in part on International Organization for Standardization and Payment Card Industry Data Security Standard guidelines, but the security landscape changes daily, so you have to go deeper than that, Parker says. “Your risk assessment has to be flexible. It sometimes has to be ad hoc, because your risk mitigation sometimes has to be ad hoc to meet those challenges.”

This is where metrics enter the picture. Here are some of the metrics Parker advises chief information security officers (CISOs) to monitor:

- **Confidential records breached or stolen.** This metric gauges access control.

“What we want to show is that we have controls in place and are managing that access, regardless of who is coming into our environment.”



KEY LESSONS

- 1 A solid, standardized framework will answer many questions about how secure you are, but tracking the right metrics will drive your understanding deeper.
- 2 Your basic message to executives should be that secure systems are what make it possible to continue growing the business.

SECURITY METRICS: THE MORE YOU KNOW, THE MORE YOU GROW

The goal, of course, is to get the number of breaches down to zero through active personal information access auditing and monitoring. “What we want to show is that we have controls in place and are managing that access, regardless of who is coming into our environment,” Parker says. “For me, access control is number one: you don’t want to give away the keys to the kingdom.”

- **Intrusion log audits.** These audits measure your understanding of which types of intrusion attempts are occurring within the security environment while also helping track time to resolution. “You want to make sure that your network team understands the intrusion attempt and is able to modify systems to defend against it,” Parker explains. If network traffic usually occurs during business hours but there’s a spike in accesses from China or Estonia at 3:00 a.m. on a Saturday, that should raise red flags. “It might be a minimal threat, it might not,” Parker comments. “The key is how quickly you can detect it and respond to it. That’s crucial.”
- **Successful malware attempts.** This metric monitors the number of malware or phishing attempts that get past filters and that staff members click. This is the “people piece” that a lot of CISOs overlook, Parker contends. “People are going to make errors; they aren’t infallible,” Parker cautions. “Security awareness really plays a large role in reducing the number of successful phishing attempts.” At Arise, he states, by monitoring this metric and fashioning an appropriate response, his team virtually eliminated successful email-based malware attacks in a little more than a year.

Parker thinks that the C suite’s comprehension of information security matters is improving. It is nonetheless important, he says, to be selective and effective at communicating data that will matter most to the leadership team. They care about what security costs now and will cost going forward, Parker notes. “You want to be able to do these things without limiting the business,” he states.

Your metrics, then, should demonstrate to leadership that secure systems make it possible to continue growing the business. “It is important to get across to the C suite that they have a secure foundation and a good security program,” he concludes. “You can grow the business knowing that those security bases are covered.”

“

It is important to get across to the C suite that they have a secure foundation and a good security program.

”



Your ability to effectively communicate your organization's risk and security posture is **critical to your success.**

Can you communicate your organization's risk and security posture in a way that executives and board members understand?



Download Now
Free Whitepaper

Read ***Managing Business Risk with Assurance Report Cards***

Align your security policies with business objectives.

Security Metrics That Drive Action in the Financial Services Industry

In this Section...



Aaron Weller
PricewaterhouseCoopers.....78



Omkhar Arasaratnam
Deutsche Bank.....85



Jason Remillard
Deutsche Bank.....80



**Troels Oerting &
Elena Kvochko**
Barclays.....87



Shawn Lawson
Silicon Valley Bank.....83

THE BEST SECURITY METRICS ARE ACTIONABLE



**AARON
WELLER**

Managing Director,
Cybersecurity & Privacy
PricewaterhouseCoopers

Aaron Weller is a managing director in PricewaterhouseCooper's (PwC) Cybersecurity & Privacy practice, with responsibility for leading this practice for the US Pacific Northwest. He has more than 18 years of global consulting and industry experience, including several years each in Europe, Australia, and the United States. Prior to joining PwC, Aaron co-founded and ran an information security and privacy strategy consulting firm and held such roles as chief information security and privacy officer for two multinational retailers.



Twitter | Website



In many ways, corporate data security is fundamentally a resource allocation issue. "There's never enough time, there's never enough money, and there's never enough people, so allocating the right dollars to protecting the most sensitive types of data is the central challenge," says Aaron Weller. To win the necessary resources, you need to align essential security goals to strategic business objectives; then, you must achieve these goals in a way that meets expectations.

An important part of accomplishing this is using the right security metrics to show what has been done and what needs to be done. But what are the metrics that resonate with board members and C-level executives? To begin with, you must use metrics that drive the right kinds of decisions and behaviors.

"A good rule of thumb," explains Weller, "is that if a metric changes and you wouldn't change your activities as a result, it's a bad metric." So, for example, you might report that you blocked 500,000 attacks on the firewall last month. That's great, but what if it was 600,000 or 400,000? Would you do anything differently? If the answer is no, there's no point in reporting that metric until it hits a trigger value when the behavior would change in response.

“ If a metric changes and you wouldn't change your activities as a result, it's a bad metric. ”

KEY LESSONS

- 1** Activity metrics are useful only to prove that you're doing something, but they don't show how effective that activity is.
- 2** Everything that gets presented to the board has to have a clear link back to business value and business strategy.



THE BEST SECURITY METRICS ARE ACTIONABLE

Weller describes three tiers of security metrics:

- **Activity metrics.** These simply provide a measure of how many times we do something or how many times an event occurs. Examples include how many vendor reviews we've done or a metric that says we doubled the number of vendor reviews in the past year. "Activity metrics can appear to be interesting," says Weller, "but they rarely if ever give us information that drives actions or behaviors. They are useful only to prove that you're doing something, but they don't show how effective or efficient that activity is."
- **Trend metrics.** Trend metrics are more informative: they can provide insight into the effectiveness of a security program. For example, if we identify 10 percent of the vendors we review as high-risk vendors, look at the average time between reviews for those vendors, then look at how that number trends, we have a metric that can be related more specifically to a particular business outcome, in this situation whether the highest risk vendors are being assessed on a cadence that is aligned with the organizations appetite for risk.
- **Outcome metrics.** "Outcome metrics are the ones that really matter to the board," says Weller. For example, an outcome metric might show how our actions actually improved the vendor-management process by eliminating risky vendors in a way that has enabled us to more effectively reach our strategic goals. Weller explains that "outcome metrics speak to the value of the activities you're performing. The executive audience is significantly more interested in the outcome than the activity itself."

Many tools are great at producing metrics, but most of those metrics are activity based. "A lot of metrics presented to the board are backwards-looking activity and trending metrics," says Weller. "What's really needed is outcome metrics and forward-looking trending metrics that indicate where we plan to be next year, which can be supported with a story on what actions will be taken to get there. That becomes the basis for decisions that shape the security program moving forward." Yet Weller says that in his experience, not enough of this kind of metric data is presented to the board in many companies. Everything that gets presented to the board has to have a clear link back to business value and business strategy.

“

Outcome metrics speak to the value of the activities you're performing.

”

BUSINESS LEADERS MUST RELATE TO YOUR SECURITY METRICS



**JASON
REMILLARD**

Vice President,
Security Architecture
Deutsche Bank

Jason Remillard is vice president, Security Architecture, at Deutsche Bank, where he is responsible for big data security and governance, risk, and compliance solutions. Previously, he was a product manager with Dell Software, managing products from the enterprise identity and access management portfolio. He has been in security for more than 20 years, including stints at IBM, Novell, Merrill Lynch, RBC, TD Bank, and Deutsche Bank. He holds an MBA from the Richard Ivey School of Business.

As vice president of security architecture for one of the world's biggest banking firms, Jason Remillard's bosses are among the planet's most sophisticated executives. When it comes to communicating with them about the security of their customers' highly sensitive information, however, Remillard has found that the universal rule applies: keep it simple, direct, and relevant.

"When you're talking risk and security, you have to spin that into the context that the executives understand," Remillard says. This insight is at the root of Remillard's choice of the metrics he monitors most closely:

- **Tracking risk vs. investment assessments.** Remillard describes this metric as a way to determine the success of investments against risks. "You have to demonstrate analysis on that," he states. "You should demonstrate that you have tracked true business risks against the investments that have been made – and that they have been mitigated appropriately." Risk-based frameworks measure the risk–reward proposition of the security investments made and help you identify the enterprise's greatest material deficiencies. From there, you can conduct control analysis followed by the actual investments. Measuring risk–mitigation is useful not only for planning your next-year budget cycle, he notes, but is also a great tool for projecting your long-range budget needs.

“When you're talking risk and security, you have to spin that into the context that the executives understand.”

KEY LESSONS

- 1 Choose metrics that you can communicate simply, directly, and cogently to busy executives, and make sure the metrics address real business issues.
- 2 If leadership can relate to your work as a CISO, you'll come out much farther ahead.



BUSINESS LEADERS MUST RELATE TO YOUR SECURITY METRICS

- **Legal compliance.** The financial services industry is highly regulated, particularly at the federal level, which has material impact on the business generally and information security particularly. The business also has to be audit- and compliance-posture ready so that it can respond to regulators' information requests. "So, that guides a lot of our investment, as well, from a security and risk-posture perspective," Remillard states. Readiness levels can be tracked and measured against industry-standard metrics established under the Control Objectives for Information and Related Technology management and governance framework, by International Organization for Standardization standards, or other relevant benchmarks, he says. This is not a case of presenting key performance indicators per se, he clarifies, "but it is gap analysis, so it's going to tell us where we have material weaknesses."
- **Interaction monitoring.** Financial institutions walk a fine line when it comes to employees' digital interactions. Clearly, digital platforms are indispensable, but Remillard warns that in the financial services space, they present huge risks for accidental or nefarious disclosure of customers' personal information. Executives need to understand which of these platforms imposes the greatest and least risks so that they can help the chief information security officer (CISO) optimally target resources. Remillard closely monitors and reports on employees' use of cloud-based services, Internet discussion forums and social networking, and software applications. "If you're in financial institutions, then there is a high risk with any of these services for regulatory fines—never mind the information-disclosure perspective," Remillard observes.

His key point is this: relate the metrics you monitor to executives' day-to-day lives. Cloud service and social media usage monitoring are great examples, he says, because executives use them, both at work and at home. Remillard offers a tip: when addressing executives, he's not averse to using props in an effort to be understood. He says that executives have no trouble wrapping their heads around massive information breaches when he tosses a USB thumb drive on the table that contains 100 million email addresses.

“

You should demonstrate that you have tracked true business risks against the investments that have been made—and that they have been mitigated appropriately.

”



BUSINESS LEADERS MUST RELATE TO YOUR SECURITY METRICS

If leadership can relate your work as a CISO to their experience as a business leader, you will come out way ahead, Remillard says. The opposite also is true. You have to contextualize the information back for the information consumer—in this case, your bosses.

“Executives would never care about a firewall administrator’s day-to-day life,” Remillard states, “but if I’m going to draw a box around using social media, that’s something that relates to them intimately.”



If you're in financial institutions, then there is a high risk with any of these services for regulatory fines—never mind the information-disclosure perspective.



COMMUNICATING SECURITY TAKES MORE THAN RAW METRICS



**SHAWN
LAWSON**

Director of Cyber Security
Silicon Valley Bank

Shawn Lawson is the director of cyber security at Silicon Valley Bank. He has worked in IT for 20 years and holds CISSP and CISM certifications, among several other IT and security certifications. During his career, he has consulted or worked for companies ranging from small startups to Fortune 50 corporations, covering almost every security technology.



Website

Shawn Lawson is the director of cyber security at Silicon Valley Bank, and he's been in the security industry for about 20 years, so he's seen a lot change and grow in the industry—including security metrics. "It's a moving target, really," he says. "Today, we're actually in the process of trying to build better metrics."

Those better metrics are designed to communicate more effectively how secure—or insecure—an organization might be. "We have metrics around security operations; the current state of things that we're working on; and things we've seen over the past few weeks, months, 90 days, or year to date," Lawson explains. "This certainly gives us a picture of our current state of health, but it doesn't necessarily give us the full picture."

To get the full picture of how secure an organization is, Lawson says you need to look beyond the metrics. "The other thing to focus on is how we compare to other institutions and also in the application of security models and standards." Lawson points to Silicon Valley Bank as an example. "We measure ourselves against the Center for Internet Security top 20 critical security controls as well as the new Federal Financial Institutions Examination Council Cybersecurity Assessment Tool. After applying these security models and standards, we can see how we rate and where we are.

“ Metrics are a moving target, really. We're actually in the process of trying to build better metrics. ”



KEY LESSONS

- 1 A set of security metrics can give you a picture of the state of your security, but it doesn't necessarily give you the whole picture. For that, use metrics to create and illustrate trends over time.
- 2 At the board level, security metrics are just noise. Instead, use those metrics to create a picture that assures the board that everything is OK.

COMMUNICATING SECURITY TAKES MORE THAN RAW METRICS

We practice defense in-depth, and we actually map that and show in our security architecture that we have multiple layers of defense. We don't rely on any one thing."

Lawson says it's also essential to stay up-to-date on the current threats in any given industry. In the financial industry, the Financial Services Information Sharing and Analysis Center is an especially important partner, because it provides cyber threat intelligence that can help Silicon Valley Bank understand the threats it's facing. It's critical, Lawson says, to understand and communicate with members of the C suite just how your security compares to existing threats and how other organizations are performing in your industry.

Raw security metrics don't always provide the information that members of the C suite need to understand risks, threats, and levels of security, however. Lawson says that his team has at times focused on metrics that don't hold a lot of value on their own. "We've done multiple rounds with some metrics that we're measuring—for example, vulnerability. Then, we look at our number of vulnerabilities and have to ask, 'What does that picture mean? Is this many vulnerabilities a good thing or a bad thing?' We have to do a calculation and benchmarking, apply the results to that number, and trend it over time. Doing so provides an indication of whether we're actually closing security risk in our environment." That, says Lawson, is how to explain levels of security to the C suite—by putting it in terms of risk and protection.

Lawson also warns security professionals to be cognizant of the different security metrics that might be meaningful to members of the C suite other than the chief executive officer. "You have different audiences. You may have security metrics that are operational, and that level of metrics is a bit more technical in nature, whereas board-level metrics would answer the question, 'Hey, we just want to know if we're secure. Paint us a picture, at a high level, that gives us some assurances that everything's okay.'"

“

We measure ourselves against the CIS top 20 critical security controls as well as the new FFIEC Cybersecurity Assessment Tool.

”



OMKHAR ARASARATNAM

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

Omkhar Arasaratnam is an experienced cyber-security and technical risk management executive, helping organizations realize their business goals while effectively managing risk and compliance requirements. He has almost 20 years of IT experience and a long history of leading global, multibillion-dollar programs. At Deutsche Bank, Omkhar is the CTO of CISO, the bank's information security department, leading CISO Strategy, architecture, and engineering. Omkhar is an 'old geek' and has contributed to the Linux kernel and helped maintained Gentoo Linux. He holds several patents and has contributed to ISO/IEC 27001:2013.

Omkhar Arasaratnam, global head of Strategy, Architecture and Engineering for CISO Cyber Security at New York's Deutsche Bank offices, states, "I think without a proper, holistic, risk-based framework, everything else is a smoke show."

His all-encompassing security mindset makes him reluctant to suggest any single group of metrics that a chief information security officer (CISO) should track to communicate effectively about information security. "What you should be concerned with is the overall risk and whether that overall risk is within tolerance," he cautions. Your particular line of business and its unique risk tolerance, therefore, should dictate the metrics you choose to track.

That said, he is comfortable listing several typical metrics that he might present to executives who express concern about enterprise-level information security—with the caveat that it is by no means comprehensive. His examples include:

- **Patch management.** For Arasaratnam, this is a compliance metric. It measures patch deployment by vulnerability severity against a predefined timeline. "What you can do is marry the significance of the patch as you have rated it with the business impact of the application on which that system runs," he explains. This data would reveal to the business team patch-time lags on any mission-critical systems. If such lags occur, he adds, "You are putting your business at more significant risk by not keeping up with the hygiene of that particular asset."

“ Without a proper, holistic, risk-based framework, everything else is a smoke show. ”



KEY LESSONS

- 1 The metrics you decide to track should be based on your particular line of business and unique risk-tolerance levels.
- 2 High-profile security lapses are big news, placing the CISO at center stage. With that raised profile comes increased responsibility.

WHEN IT COMES TO SECURITY METRICS, GET S.M.A.R.T.

- **Mean time to incident resolution.** Measured by severity rating, this is another important metric, Arasaratnam states. “It tells you that a severity has been assigned to it (an incident)”. It also informs you as to how quickly you can expect this issue to be resolved, based on its severity. Similar to the data on the patch dashboard mentioned earlier, he adds, tracking incident-resolution time can suggest whether the business needs to enter into service quality improvement to address areas they are lagging. “I think that is an effective metric to capture,” he observes.
- **Security posture compliance.** Let’s say your security policy dictates that no Windows Server instance can host open, unauthenticated file shares. You would conduct a scan to validate that, Arasaratnam says. The resulting measurement would tell you how many devices are conforming to your standards. “It tells you whether what you have written down as security standards are actually being enacted,” Arasaratnam adds.

Some metrics can be red herrings, he notes. He doesn’t typically track the raw number of hits on his intrusion-detection technologies, for example. “The reason I say that,” he explains, “is because no one can fundamentally tell you if a trend going up or going down is a good thing.”

When it comes to communicating data with executives, Arasaratnam advises against “info-glut.” He recalls working with an organization that routinely issued 200-page monthly security reports. “If the information is that dense,” he warns, “people aren’t going to be able to take action on things.”

His advice: get S.M.A.R.T. “You need to have metrics and messages across security that are specific, measurable, attainable, relevant, and time-bound,” he says. “If you don’t, you’re going to lose your audience.”

Security lapses in the business world are big news these days, placing the CISO at center stage. With that raised profile, Arasaratnam cautions, comes increased responsibility to prove your value, he says—not that it should be difficult.

“We are giving them the tools to allow them to make those risk-based decisions about our business and to ensure that we have stayed within an acceptable risk tolerance,” Arasaratnam states. “It’s always about being able to establish the appropriate level of risk that we as a business are willing to tolerate.”



You need to have metrics and messages across security that are specific, measurable, attainable, relevant, and time-bound.



FOR FINANCIAL SERVICES, SECURITY MEANS TRUST



TROELS OERTING

Group Chief Information Security Officer
Barclays

Troels Oerting, CISO at Barclays, has more than 35 years' experience in Law Enforcement - the last 15 in senior management positions in Danish and International police organizations, with a focus on ICT security. He is the former director of Danish NCIS, the National Crime Squad, SOCA and the director of operations in the Danish Security Intelligence Service.



Twitter



ELENA KVOCHKO

Head of Global Information Security Strategy and Implementation
Barclays

Elena Kvochko is the head of global information security strategy and implementation at Barclays, a multinational banking and financial services company.



Twitter

The ability to define a security posture has become critical to the financial services segment in recent years. "Banks and financial services institutions understand that the main product they sell is trust," explain Troels Oerting and Elena Kvochko.

"Without trust, they cannot sustain customer loyalty," says Kvochko. In this industry segment, customer loyalty and trust come through innovation, privacy, security, convenience, and speed to market. All those factors work together to drive the business and provide competitive advantage. Speaking about their industry, Oerting and Kvochko said that for many organizations, quantifying their security posture isn't easy due to lack of data and visibility. "You don't know what you don't know."

“Banks and financial services institutions understand that the main product they sell is trust.”

KEY LESSONS

- 1 With the right metrics, it's possible to construct a security posture that weighs controls against assets against vulnerabilities.
- 2 One area that is becoming increasingly important to both financial services and regulators has to do with third- and fourth-party vendor assurance.



FOR FINANCIAL SERVICES, SECURITY MEANS TRUST

The best place to start is with assets. “Complete asset inventory includes prioritizing core assets that support the unique value of your business,” Oerting states. For most companies, this inventory includes elements like email, business strategies, customer account information, employee and client files, financial information, and intellectual property that make the company competitive. Metrics might include costs to acquire and brand value.

Next, you must review the controls you have in place. Controls enhance the business’ ability to protect, predict, and respond to cyber-threats. “It’s important to have a clear view of the safeguards you have in place around your assets,” says Kvochko. Metrics that provide a view of controls include hardware and software systems and their security update status, as well as employee security awareness metrics.

Finally, you must look at your vulnerabilities, which can include their severity, how long it takes to eliminate them, and response time. This kind of information can come from red teaming and pen testing.

“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,” says Oerting.

One area that is becoming increasingly important to both financial services and regulators has to do with third- and fourth-party vendor assurance. According to Oerting and Kvochko, “It’s not only about your own controls. Do you know everyone who has access to your systems, how they protect their systems, who holds your data and how they protect it, or all the applications the data has passed through?”

These questions are often difficult to answer, and because it’s such a new area, there are no established metrics. Oerting says, “This is an area where we can definitely work together as an industry to develop better visibility”.

“

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.

”



Tenable Network Security 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 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, by visiting tenable.com.

To learn more about how Tenable Network Security can help you use metrics and report cards to demonstrate security assurance in ways executives can understand, go to <http://tenable.com/driveaction>