



# Communicating Security Program Effectiveness to Executives and the Board

Quotes from 33 Experts



**tenable**<sup>®</sup>  
network security

# 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](https://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 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.



**GARY  
HAYSLIP**

Deputy Director/CISO  
City of San Diego, CA

   
Twitter | Website

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

**Metrics are great, but only if they mean something to your business. With respect to cybersecurity, three metrics—time to detect attacks, time to contain damage from those attacks, and the number of systems an attack compromises—can tell you how much work is yet to be done to better secure your organization's network.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**BEN  
ROTHKE**

Senior eGRC Consultant  
Nettitude Ltd.

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

CEOs want their company to be in *The Wall Street Journal* because of record profits, not because of a data breach. Most CEOs' eyes glaze over when the security discussion is too technical, so it's important that CISOs know how to convey their security strategy and rationale without delving too deeply into the technology or the nuts and bolts of how they make the business secure.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**PRASANNA  
RAMAKRISHNAN**

VP, Information  
Risk Management  
Career Education Corporation

---

 Tweet this Quote

 Share on LinkedIn

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

**Rather than focusing on metrics and numbers whose meaning may not be clear, CISOs should identify trends, explain how they arose, and recommend specific courses of action to address them. By presenting a careful, nuanced approach, CISOs can help CEOs and board members make strategic decisions about business risks.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**DAVID  
MACLEOD**

Vice President, CIO/CISO  
Welltok



Website



Tweet this Quote



Share on LinkedIn

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

**When the CEO asks how secure the company is, it's important to give him or her confidence that the security team has made the appropriate plans in advance, knows what measures to take in the event of an incident, and is clear on how to respond immediately should it take place. That's how the CEO knows how secure the business is.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**KEYAAN  
WILLIAMS**

Senior Executive, CCSIO  
Programs  
EC-Council

   
Twitter | Website

 Tweet this Quote

 Share on LinkedIn

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

Metrics play a key role in effective communication between the CISO and C-level executives. By carefully and intelligently choosing the metrics that are most important to your particular business and avoiding those that aren't, you can better detect security patterns, spare your organization needless disruption, and show company executives that your office is on the ball.



Want to read more?  
[Download the full eBook Free >](#)

About the Author: 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.



**NIKK  
GILBERT**

Director of Global Information  
Protection and Assurance  
ConocoPhillips

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

“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.”

The secret to success as a CISO is to forge relationships, and metrics can be a great way to solidify those relationships. The CISO needs to understand how to simply and effectively communicate security metrics to many different audiences. When the CISO secures the support of the team, it’s then crucial to continue showing the value of his or her security program. Measuring metrics, both at the operational and strategic levels, is vital to that task.



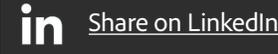
**Want to read more?**  
**Download the full eBook Free >**

**About the Author:** 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.



**ADAM  
ELY**

CSO and Co-founder  
Bluebox Security



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

Company executives are inundated with data from all the departments that report to them, so giving them the wrong metrics is just noise. Instead, present metrics that tell executives a story. Look for any indicator that the business is progressing or slipping. Then, use that information along with metrics from the industry to understand what constitutes the norm and what the executives can expect.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



## 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.



**TIM  
PRENDERGAST**

CEO  
Evident.io

    
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

CEOs demand two answers from their security leaders: “Is our security getting better or worse?”, and “Are we adhering to our security strategy?” To that end, two important areas in which to focus your metrics are how many breaches have been associated with new technologies your organization has released and how security-minded your third-party vendors are.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**CHARLES  
THOLEN**

Owner and CEO  
Cognoscape LLC

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

There's no simple answer to the question of how secure a company is because the answer always depends on the maturity of an organization's approach to its security strategy. As a company develops and implements its security program, it must also develop metrics that provide visibility into the effectiveness of that program, such as compliance or patch management. The metrics that are most useful to a CEO relate to how close the security program is to achieving its goals.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**DANIEL  
RIEDEL**  
CEO  
New Context

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

To make the best financial decisions for the organization, the business decision makers must understand the security risks that the organization faces. To give the CEO and board the information they need to allocate resource to secure the enterprise infrastructure, the security organization must look at risk from two perspectives: the value of the company's data to potential thieves and the value of those data to the business itself.



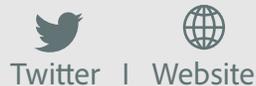
Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**ROBIN "MONTANA"  
WILLIAMS**

Senior Manager, Cybersecurity  
Practices & Cyber Evangelist  
ISACA



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

Careful risk assessment and a clear path to addressing your organization’s risk can give you a strategic roadmap for establishing 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.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**JAKE  
KOUNS**

CISO  
Risk Based Security

    
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

With more and more companies depending on outsourced products and services, vendors become a source of potential vulnerability. To ensure that those relationships don’t endanger your organization, it’s important to measure the risk that each vendor poses and balance that risk against the value of the strategic relationship.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



CHRIS  
MARK

   
Twitter | Blog



Tweet this Quote



Share on LinkedIn

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

Security isn't an either/or proposition. The question of how secure we really are can be answered only in the context of identified risk. In the end, 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.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



## ANDREW STORMS

Vice President,  
Security Services  
New Context



Twitter



Website



Blog



Tweet this Quote



Share on LinkedIn

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

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 and 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. By agreeing ahead of time which metrics are most important across executives, companies can improve their security profile dramatically.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**GENADY  
VISHNEVETSKY**

CISO  
Stewart Title Guarantee  
Company



Website



Tweet this Quote



Share on LinkedIn

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

**Your CEO isn't interested in how many vulnerabilities you have. That's not to say that the number of vulnerabilities isn't important, just that when you're communicating the strength of corporate security to C suite executives, such metrics won't provide useful information. Instead, select a few metrics that are both qualitative and quantitative. At the end of the day, executives understand the risk to the business.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**TREVOR  
HAWTHORN**

CTO  
Wombat Security  
Technologies

 |  |   
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

**There was a time when information security was something you added to the business—an extra layer of protection, like insurance. That’s no longer the case. Today, security is baked into business operations, so executives want to know if the business is safe. To work in the boardroom, metrics must encapsulate the business’ security posture, and that means that metrics must be validated.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**SCOTT  
SINGER**

CISO  
PaR Systems, Inc.

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

“ 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 CEO- and board-level presentations, you must use security metrics carefully. 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. To be effective, it's important to raise issues using a risk-based language that allows the board to make risk-based decisions on cyber-security spending.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**ROY  
MELLINGER**

VP, IT Security, and CISO  
Anthem, Inc.



Tweet this Quote



Share on LinkedIn

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

**You can't control what you don't understand, you can't manage what you don't measure, 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.**



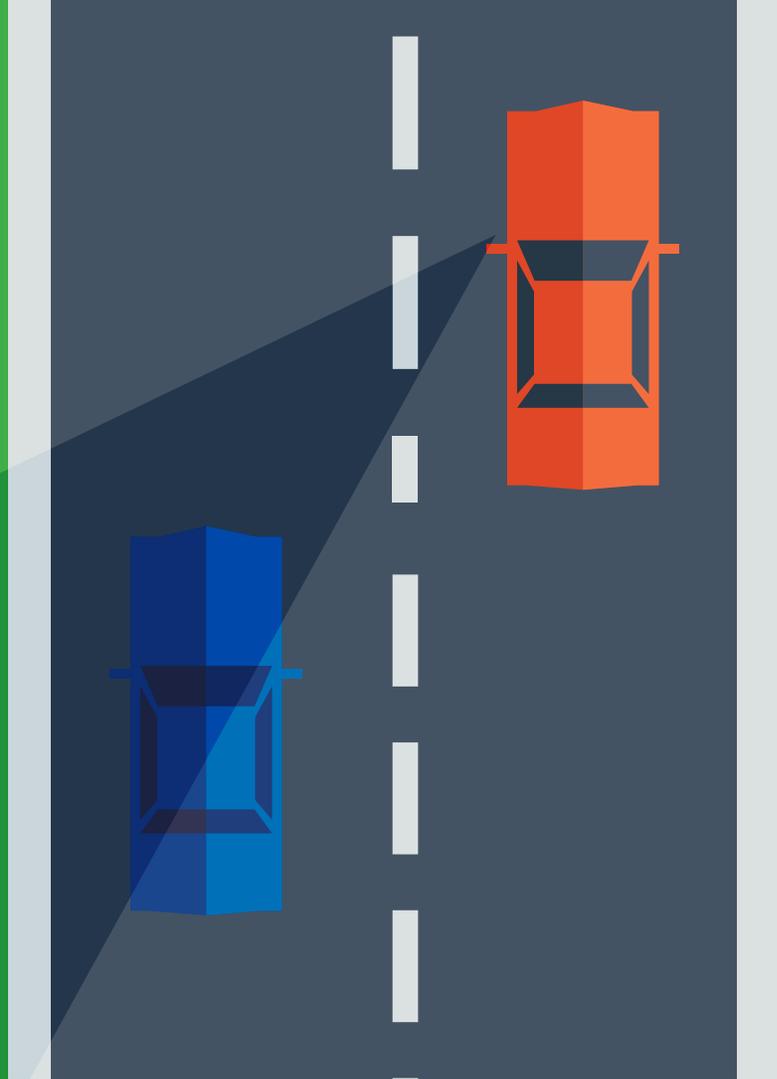
**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



# 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.



**AANCHAL  
GUPTA**

CISO, Skype  
Microsoft

 |  |   
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

C suite executives appreciate anyone who can get to the point of any discussion quickly and efficiently. CISOs should embrace that idea when they're choosing the metrics they will provide to leadership. Trends over time, penetration testing results, and engineering security maturity go a long way toward demonstrating that you've done your homework.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**JONATHAN  
CHOW**

Senior VP, CISO  
Live Nation Entertainment



Tweet this Quote



Share on LinkedIn

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

When building a security program, macro-level metrics can be extremely useful. Rather than measuring the total number of vulnerabilities, for example, consider measuring the *average* vulnerabilities per end point. By looking at security from a hire-level perspective, you can better determine whether and to what extent your organization is struggling.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**VIKAS  
BHATIA**  
CEO & Founder  
Kalki Consulting

    
Twitter | Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

Most security organizations still perceive the security problem as an outside-in problem. If, however, you view it as having three parts—external threats, internal threats, and technical misconfigurations or coverage gaps—collect metrics for each, then look at the components as a whole, you can better quantify risks and assess their potential impact on the organization.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**JULIAN  
WAITS**  
CEO  
PivotPoint Risk Analytics

   
Twitter | Blog

 Tweet this Quote

 Share on LinkedIn

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

As a CISO, you must not only communicate security risks in a language that your CEO and other executives will understand but also protect the CEO from him- or herself in cases of phishing attacks and the like. To that end, be prepared to answer your CEO’s questions using metrics on the applications, processes, and end users that matter most.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**J. WOLFGANG  
GOERLICH**

Director of Security Strategy  
CBI  
(Creative Breakthroughs Inc.)



Twitter



Website



Blog



Tweet this Quote



Share on LinkedIn

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

To determine whether your company is secure, you must take a pragmatic look at your controls and the real threats you face. For an accurate assessment, you need quality intelligence—intelligence about your internal state, what’s happening across your industry, and which threats may target your particular organization.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**DAVE  
SHACKLEFORD**

CEO  
Voodoo Security

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

“ 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. ”

**Business is a language of measurable metrics. Any competent CISO can offer up metrics that help shape the C suite's understanding of IT security and score resources needed to protect the environment, but select those metrics with purpose.**



**Want to read more?**  
**Download the full eBook Free >**

**About the Author:** 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.



**ED  
ADAMS**

CEO  
Security Innovation, Inc.

 |  |   
Twitter | Website | Blog

 Tweet this Quote

 Share on LinkedIn

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

When evaluating your organization's security posture at a high level, consider collecting information and metrics that answer three key questions: How well patched are your systems? Do you filter all email that originates from email servers that are less than two days old? And finally, what percentage of your software engineers have gone through security training and received an acceptable assessment score?



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**ROOTA  
ALMEIDA**

Head of Information Security  
Delta Dental of New Jersey



Tweet this Quote



Share on LinkedIn

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

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. Security teams in the past focused on preventing penetration into systems that contained sensitive data, but today, more emphasis is placed on better detection and mitigation. 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 that, you need the right kinds of security metrics.



Want to read more?  
**Download the full  
eBook Free >**

**About the Author:** Rooter 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. Rooter 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.



**STEVEN  
PARKER**

Senior Director,  
Information Security  
The Advisory Board Company

   
Website | Blog

 [Tweet this Quote](#)

 [Share on LinkedIn](#)

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

**At most companies, the C suite's comprehension of information security matters is improving. Nevertheless, it's important for CISOs to be selective and effective at communicating data that will matter most to the leadership team. Your basic message to executives should be that secure systems are what make it possible to continue growing the business.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



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.



**AARON  
WELLER**

Managing Director,  
Cybersecurity & Privacy  
PricewaterhouseCoopers



Twitter | Website



Tweet this Quote



Share on LinkedIn

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

In many ways, corporate data security is fundamentally a resource allocation issue. There's never enough time, money, or people, so allocating the right dollars to protecting the most sensitive data is the central challenge. 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.



Want to read more?  
[Download the full eBook Free >](#)

**About the Author:** 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.



**JASON  
REMILLARD**

Vice President,  
Security Architecture  
Deutsche Bank



Tweet this Quote



Share on LinkedIn

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

**When it comes to communicating with top executives about the security of their customers' highly sensitive information, the universal rule applies: keep it simple, direct, and relevant. Relate the metrics you monitor to executives' day-to-day lives. Cloud service and social media usage monitoring are great examples because executives use them, both at work and at home. If leadership can relate to your work as a CISO, you'll come out ahead.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**SHAWN  
LAWSON**

Director of Cyber Security  
Silicon Valley Bank



Website



Tweet this Quote



Share on LinkedIn

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

**To get the full picture of how secure an organization is, you need to look beyond the metrics. How does the company compare to other institutions and in the application of security models and standards? 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, you must use metrics to create and illustrate trends over time.**



**Want to read more?**  
**Download the full eBook Free >**

**About the Author:** Shawn Lawson is the directory 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.



**OMKHAR  
ARASARATNAM**

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

---



Tweet this Quote



Share on LinkedIn

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

**High-profile security lapses are big news, placing the CISO at center stage. With that raised profile comes increased responsibility, but metrics and messages across security that are specific, measurable, attainable, relevant, and time-bound contribute to maintaining a holistic, risk-based framework for your business.**



**Want to read more?  
Download the full  
eBook Free >**

**About the Author:** 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.



**TROELS OERTING**

Group Chief Information Security Officer  
Barclays



Twitter



**ELENA KVOCHKO**

Head of Global Information Security  
Strategy and Implementation  
Barclays



Twitter



Tweet this Quote



Share on LinkedIn

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

**Banks and financial services institutions understand that the main product they sell is trust. With that in mind, financial services organizations must assess their security posture in terms of privacy, security, convenience. With the right metrics, it's possible to construct a security posture that weighs controls against assets against vulnerabilities.**



**Want to read more?  
Download the full  
eBook Free >**

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



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](http://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>**