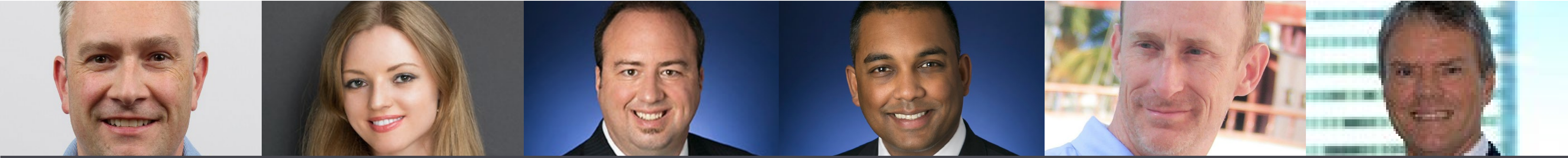


Mighty Guides

Using Security Metrics to Drive Action

Security Metrics That Drive Action in the Financial Services Industry

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

tenable® network security

FOREWORD

Security has come a long way, but it continues to face two significant challenges: the continuous evolution and adaption 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

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

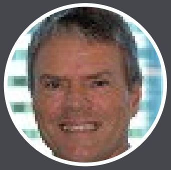
Mighty Guides make you stronger.

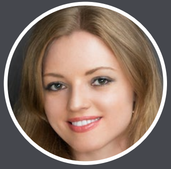
These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of 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.

© 2016 Mighty Guides, Inc. I 62 Nassau Drive I Great Neck, NY 11021 I 516-360-2622 I www.mightyguides.com

Security Metrics That Drive Action in the Financial Services Industry





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

MightyGuides
Using Security Metrics to Drive Action
33 Experts Share How to Communicate Security Program Effectiveness to Business Executives and the Board
tenable network security

Download the full e-book:
USING SECURITY METRICS TO DRIVE ACTION

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.

Weller describes three tiers of security metrics:

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.**

> *"If a metric changes and you wouldn't change your activities as a result, it's a bad metric."*

- **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."

> “*Outcome metrics speak to the value of the activities you're performing.*”

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.

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.

Using Security Metrics to Drive Action

tenable

Download the full e-book:
USING SECURITY METRICS TO DRIVE ACTION

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."

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.**

> *"When you're talking risk and security, you have to spin that into the context that the executives understand."*

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.

- **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.

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

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.

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 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.

Website

Using Security Metrics to Drive Action

tenable

Download the full e-book:
USING SECURITY METRICS TO DRIVE ACTION

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."

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.**

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

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. 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.

MightyGuides

Using Security Metrics to Drive Action

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

tenable network security

Download the full e-book:
USING SECURITY METRICS TO DRIVE ACTION

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.

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.**

> *"Without a proper, holistic, risk-based framework, everything else is a smoke show."*

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."

- **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."

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

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.”

> “It's always about being able to establish the appropriate level of risk that we as a business are willing to tolerate.”

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

Download the full e-book:
USING SECURITY METRICS TO DRIVE ACTION

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."

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.**

> *"Banks and financial services institutions understand that the main product they sell is 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

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.

MEET TENABLE

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.

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