Mighty Guides

Using Security Metrics to Drive Action

Security Metrics That Help Boards Assess Risk

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

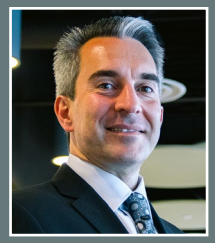
tenable® network security

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

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.

tenable®
network security

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

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

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

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.

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.**

> *"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?"*

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

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. 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.

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

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.

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

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

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."

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.**

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."*

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.

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

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 pursing and winning new business opportunities, and that discussion will be of great interest to the CEO.

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

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

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.

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.**

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

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:

- **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.

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

"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.

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

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

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

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

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.

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.**

> *"Many people say, 'Our front door is locked and now we're safe.' I say to them, 'But what about all your vendors?"*

TO BE THOROUGH, INCLUDE VENDOR SECURITY METRICS

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."

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.

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

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.

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.

Twitter | Blog

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

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 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;

> *"As important as compliance is, being compliant does not equate to being secure."*

- Show your compliance standing;
- 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.

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

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.

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

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

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.

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.**

> *"We need to agree on the metrics that make the most sense to everybody across the entire C suite."*

DEFINE SECURITY METRICS THAT ARE VALUABLE ACROSS THE C-SUITE

"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."

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 Guarantee 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

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

"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.

> *"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

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.

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."

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

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."

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

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

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.

> *"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.**

- **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.
- **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.

> *"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."*

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.

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

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

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.

> *"If I start using technical security terms and metrics, I completely lose the audience."*

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.**

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."

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."*

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.

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

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.

> *"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

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?"

- **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."*

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."*

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 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