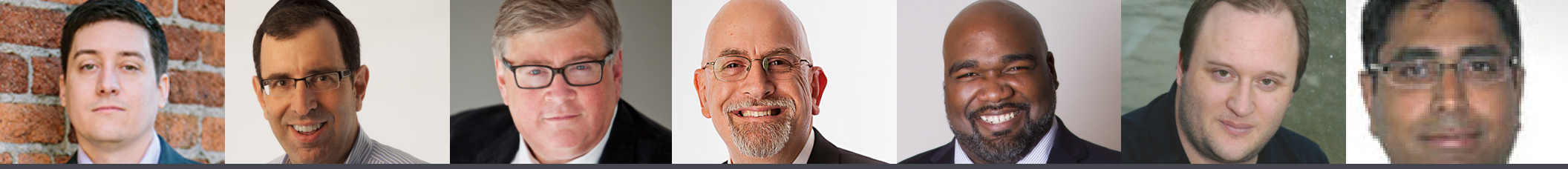

Mighty Guides

Using Security Metrics to Drive Action

Security Metrics That Tell a Story to the Board

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

tenable™

FOREWORD

Today's cybersecurity challenges are more complex than ever before. Technologies like Development Containers, Cloud, BYOD, and BYOA have greatly complicated the security team's ability to understand all of the potential IT attack surface. And while you may have the budget dollars to invest in new cyber technologies, the size and workload of your security team is a key gating issue. The core foundation of a successful cybersecurity program requires that you understand all of the IT assets operating against your environment, both inside and outside of your network, identify and remediate vulnerabilities, and continuously assess and measure risk.

Although organizations are investing more of their IT budget on cybersecurity technologies, high-impact breaches continue to make headlines. As a result, senior business executives and board members are asking security teams tough questions about the effectiveness of their security controls -- and how they are measuring, getting control of, and reporting on cyber risk.

At Tenable, we partnered with the team at Mighty Guides to ask senior security industry leaders the following questions: "Your CEO calls and asks, 'How exposed are we, and how secure is our organization?' What strategies and metrics do you use to answer?" We compiled their responses into this e-book -- giving you useful insights from your peers on how they answer these tough questions -- so that you can be prepared when asked yourself.

While every organization is different and has its own unique challenges and constraints, CISOs must deliver answers that are metrics driven, benchmarked to industry best practices and standards, defensible and approximate reality.

We hope you find this e-book useful in helping you develop and communicate security metrics in your own organization. And in follow on parts of this series, we will share with you additional market research that we know you will find compelling and useful when communicating the effectiveness of your cyber security program to your C-suite and Boards.

Regards,
Amit Yoran
Chairman and Chief Executive Officer, Tenable Network Security

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. Learn more at 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.

Security Metrics That Tell a Story to the Board

GOOD SECURITY METRICS ARE A WORK IN PROGRESS

GARY HAYSLIP

Deputy Director/CISO
City of San Diego, CA

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

Twitter | Website

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

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

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

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

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

> *"When you collect metrics, you're collecting them to tell a story."*

KEY LESSONS

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

GOOD SECURITY METRICS ARE A WORK IN PROGRESS

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

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

> *"The metrics you collect need to mean something to the organization."*

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

Not all metrics are created equal, of course. Hayslip used to monitor the number of help desk tickets that employees filed. That proved not terribly useful. "They could be submitting requests to my team's email box that don't even apply to us, just hoping someone is going to help them," he explains. In the end, Hayslip counsels CISOs to choose which metrics to track based not on their personal curiosity but on their business' bottom line. "The metrics you collect need to mean something to the organization," he says.

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

CEOS REQUIRE SECURITY METRICS WITH A HIGH-LEVEL FOCUS

BEN ROTHKE

Senior eGRC Consultant
Nettitude Ltd.

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

Twitter | Website | Blog

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

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

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

KEY LESSONS

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

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

CEOS REQUIRE SECURITY METRICS WITH A HIGH-LEVEL FOCUS

Several metrics Rothke finds useful under the right circumstances are:

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

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

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

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

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

PRASANNA RAMAKRISHNAN

VP, Information Risk Management
Career Education Corporation

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

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

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

For example, he says, "I would say that the trend we see is that we're slow in reducing our lead time between identifying vulnerabilities and fixing them, and we need to speed that up."

KEY LESSONS

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

> *"If you say you patched 3,732 vulnerabilities last month, what does that mean to a CEO?"*

When explaining why the security team is slow to fix vulnerabilities, this might mean sharing that they have been assigned other, conflicting priority projects that have taken up staff time, reducing the personnel available to address vulnerabilities. Recommendations for addressing that resource problem might involve automating a process or employing more people. Rather than talking about pure security statistics, this is the type of discussion that needs to happen with the CEO.

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

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

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

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

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

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

USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN

DAVID MACLEOD

Vice President, CIO/CISO
Welltok

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

Website

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

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

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

KEY LESSONS

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

> *"That's how they'll know how secure we really are, because it is not a question of if, but rather of when a malicious event will occur."*

USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN

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

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

The human component of security is also important to highlight, so MacLeod presents statistics around people and their level of security awareness. "We have an active security awareness campaign on which I provide the board with statistics so that they know what we're doing to keep our workforce informed."

"This way, we can make sure that they're looking at things from a security or privacy perspective," he says. MacLeod shares data ranging from the relative strength of passwords employed by the workforce to how many people have completed his security awareness training, how many haven't, and how many people require more assertive follow-up to ensure their participation.

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

USE SECURITY METRICS TO PRESENT A STRONG ACTION PLAN

MacLeod's team spends a lot of time sending out security alerts to the company's workforce warning them about some of the scams the Internal Revenue Service has been reporting on, for example. "If I can get them to think about protecting their personal information, it's easy to get them to care about protecting company information," he says. "We don't just worry about telling them how to protect the company assets. We want them to always think about things with a mind on security, privacy, and protection of information—no matter who information belongs to." With so many employees working from home or telecommuting, using their own equipment and network to access company resources, this awareness becomes even more crucial.

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

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

KEYAAN WILLIAMS

Senior Executive,
CCSIO Programs
EC-Council

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

Twitter | Website

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

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

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

- **Access control.** How often, through what means, and when are people accessing your network? These metrics show whether you are effectively preventing unauthorized network access while allowing reasonable and authorized access. "Is there some kind of anomaly?" he asks. "Is there an administrator logging on in the middle of the night for some reason that makes no sense?"

KEY LESSONS

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

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

Be smart and flexible in responding to these metrics, however. If a particular data modeler tends to log on in the middle of the night to work out solutions, you should be able to spot that trend. You don't want to block that kind of productive activity. Of course, if you see that someone has tried and failed to log on 700 times, you might want to call on your rapid response team.

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

Whether you follow Williams' specific advice or not, the point is to be intelligently selective. Follow the metrics that are most important to your particular business. Don't waste your time on pointless measurements.

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

In a previous CISO job, for instance, Williams was required to monitor Microsoft SharePoint server accesses. Nothing was ever done with the information—a total waste of time and resources.

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

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

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

GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST

NIKK GILBERT

Director of Global Information Protection and Assurance
ConocoPhillips

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

Twitter | Website | Blog

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

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

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

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

KEY LESSONS

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

> *"What I'm trying to do from a strategic point of view is find those metrics that are really going to resonate with the business."*

GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST

"There are so many metrics out there that you can use to show different things," he says. "What I'm trying to do from a strategic point of view is find those metrics that are really going to resonate with the business."

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

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

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

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

GOOD SECURITY METRICS BUILD RELATIONSHIPS AND TRUST

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

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

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

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

> *"Executives don't want to hear about servers, and the security analysts don't want to talk to the executives. So I guess I'm a universal translator."*

CHOOSE SECURITY METRICS THAT TELL A STORY

ADAM ELY

CSO and Co-founder
Bluebox Security

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

Twitter | Website

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

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

Ely says, "I'm looking for any indicator that tells me that we're progressing or slipping. Then, I'm going to use those things along with metrics from the industry to understand what constitutes the norm and what we can expect."

> *"Look at data around probabilities of compromise and specifically at where issues occurred in the past."*

KEY LESSONS

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

CHOOSE SECURITY METRICS THAT TELL A STORY

He uses this information to build a full answer to take to the C suite that provides solid, quantifiable information about how the organization is getting better over time. "Or we're not. Whatever the answer is," says Ely. "Here's the area that we really need to focus on, and here's the level of effort we need to apply. It's about connecting the dots."

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

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

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

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

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

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 global public sector, to mid-sized enterprises 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 tenable.com/solutions/security-assurance