Mighty Guides

Using Security Metrics to Drive Action

Security Metrics for Threat Management

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

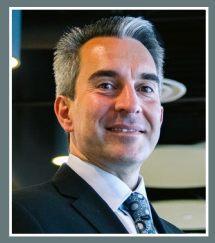
tenable® network security

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 for Threat Management

AANCHAL GUPTA

CISO, Skype
Microsoft

Aanchal Gupta leads a team of experts at Microsoft in the areas of security, privacy, and compliance. She is passionate about building products that are safe, trustworthy, and accessible to everyday users. Prior to joining Microsoft, Aanchal led Yahoo!'s Global Identity team, contributing to various authentication and authorization open standards such as OpenID and OAuth. She has more than two decades of experience leading large, distributed development teams developing global software used by millions.

Twitter | Website | Blog

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

Aanchal Gupta empathizes with C suite executives' need to get to the point of any discussion. As chief information security officer (CISO) for Skype and Skype for Business, she appreciates terseness from her own team.

When an executive asks her for an enterprise security update, she shows the same courtesy. That attitude helps guide her selection of metrics to illustrate business-risk assessments to senior leaders. Examples of those metrics include:

- **Externally reported security incidents.** Because Skype is a public-facing, Microsoft-owned communications platform, external researchers do a lot of testing on Skype. "Anything that is reported is taken very seriously. We track these issues closely," Gupta says. She graphs incidents over time, she states, to help leadership understand whether Skype is addressing these potential vulnerabilities. She also tracks the mean time to resolve each issue. If, over time, both graphs do not trend downward, she notes, "Then something is wrong—we are not focusing our engineering investments in the right places."

> *"Right away you get four follow up meeting invitations from the engineering managers: 'Can you walk my team through why we are red and how we can get to green?'"*

KEY LESSONS

1. **Tracking externally reported incidents will help you determine whether your security preparedness is trending in the right direction.**

2. **Don't try to tell the whole story verbally. A data-rich trend graph can be much more compelling and convincing than any speech.**

WITH SECURITY METRICS, EVERY PICTURE TELLS A STORY

- **Penetration testing.** Skype regularly pen-tests its own product, Gupta notes, and this metric reveals any visible gaps. "I try to categorize those gaps for our leadership team," she adds. Skype uses Microsoft's "STRIDE" model to categorize threats—an acronym that stands for "spoofing identity," "tampering with data," "repudiation threats," "information disclosure," "denial of service" and "elevation of privilege." The metric is important to senior leadership, Gupta asserts, because they know that penetration failures can be prevented with more in-depth training.
- **Engineering security maturity.** Gupta believes that when engineers understand that they're responsible for security from the requirements phase all throughout the development process, the final product is more secure. That's why threat modeling is required of the Skype engineering teams. She uses color-coded heat maps to track teams' relative security-preparedness ranking graphically, she says. The best prepared fall into the green zone; the least prepared are color-coded red. This is a simple way to communicate to executives which engineering teams need "encouragement" to focus more on security. "You can see the wheels moving right away," she comments. "You leave the executive meeting and right away you get four follow up meeting invitations from the engineering managers: 'Can you walk my team through why we are red and how we can get to green?'"

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

It is important for CISOs to avoid presenting prebaked metrics to executives, Gupta cautions. If at an executive meeting you point out that the organization has several open security issues, someone will ask you to prioritize and rank them. If you reply that some of the issues you have charted have not yet been severity-ranked, leadership will not be happy.

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

A final insight: a picture is worth a thousand words, especially one that illustrates your metrics in an effective and cogent way. "You may speak for an hour and nobody will believe that you have affected the problem," Gupta contends. "But if you show leadership a trend graph, they'll be convinced."

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

JONATHAN CHOW

Senior VP, CISO
Live Nation Entertainment

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

Twitter

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

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

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

- **Average vulnerabilities per end point.** You naturally want to know the relative vulnerability of your enterprise computers, company-issued mobile phones and tablets, and other end-user systems, Chow says, but unless you put that into context, you could easily get a skewed view.

> *"We started to make it higher level. We weren't focusing so much on specific vulnerabilities."*

KEY LESSONS

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

Measuring in terms of average per device is a great way to get a grip on the relative security of the enterprise, Chow says. You might find your average vulnerability per system was 24 last year, and this year it's down to two, for instance. "That is a metric I would bring up to the chief executive officer and to the board," he says.

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

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

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

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

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

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

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

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

VIKAS BHATIA

CEO & Founder
Kalki Consulting

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

Twitter | Website | Blog

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

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

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

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

KEY LESSONS

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

> *"Many technical CISOs are unable to quantify the impact of a risk to the business."*

THE KEY: LINKING SECURITY METRICS TO BUSINESS OBJECTIVES

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

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

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

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

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

JULIAN WAITS
CEO
PivotPoint Risk Analytics

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

Twitter | Blog

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

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

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

- **Patch rates.** Time to deploy or update mission-critical applications and operating systems in devices that are attached to the network is a key metric, Waits asserts. Using technologies like Tenable SecurityCenter, he says, you can measure this time easily.

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

KEY LESSONS

1. **The CISO should be prepared to answer a CEO's questions using metrics on the applications, processes, and end users that matter most.**

2. **The CISO must play educator to the CEO as well as the other key end users. Metrics are an important way to ensure that the word is getting out.**

"As the environment changes, as you add new applications to the environment, you should be continuously monitoring updates," he suggests.

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

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

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

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

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

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

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

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

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

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

J. WOLFGANG GOERLICH

Director of Security Strategy
CBI
(Creative Breakthroughs Inc.)

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

Twitter | Website | Blog

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

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

When evaluating your internal state, Goerlich recommends considering security metrics, such as the types of attacks you're seeing at the moment and where they are originating, and assessing the type of projects your staff are working on that might encourage those types of attacks. You can find these metrics by tapping your systems for internal intrusion detection and prevention, data loss prevention, vulnerability management, and security information management.

KEY LESSONS

1. **To determine the best security metrics for your organization, gather quality intelligence on the internal and external threats unique to your environment.**

2. **When communicating your company's security posture to the CEO, use specific examples that are supported by data and actionable.**

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

With your internal metrics in place, use them to spot trends that indicate what types of attacks are commonly happening internally. Map those trends, threat-model them, then outline your detective and preventative controls for those kinds of attacks.

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

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

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

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

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

prevent and detect this type of attack.

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

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

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

DAVE SHACKLEFORD
CEO
Voodoo Security

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

Twitter | Website | Blog

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

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

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

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

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

> *"If you tell business people, 'Hey, look at all these systems that have antivirus!' Who cares? What does that even mean to me?"*

KEY LESSONS

1. **Choose metrics purposefully. Tracking unapproved configuration changes makes sense; tracking the number of antivirus installations probably doesn't.**

2. **CISOs should constantly chart their IT environment and keep tracked metrics close at hand, to be communicated at a moment's notice.**

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

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

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

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

GOVERNMENT AGENCIES RELY TOO HEAVILY ON COMPLIANCE

ED ADAMS

CEO

Security Innovation, Inc.

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

Twitter | Website | Blog

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

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

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

KEY LESSONS

1. **Software is now running our world. If we don't create and deploy secure software, we are creating massive attack surfaces for ourselves.**

2. **Most government agencies are not driven by a need to achieve a certain security posture. Rather, they're driven by mandates to be compliant with security standards.**

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

GOVERNMENT AGENCIES RELY TOO HEAVILY ON COMPLIANCE

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

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

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

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

ROOTA ALMEIDA

Head of Information Security
Delta Dental of New Jersey

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

Twitter

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

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

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

- **Metrics and trends that show what kinds of malicious content the system is blocking**. "If you detect an upward trend in a particular kind of attack, you can apply analytics to get a better sense of what's happening, whether it's something new or related to other attacks you're experiencing," says Almeida.

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

KEY LESSONS

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

- **Metrics and trends that show how much malicious content is not getting blocked.** This is malicious content that slips through, creating incidents that require resolution. These are not necessarily big incidents, but they include everything that's not being blocked.
- **Metrics and trends on time between detection and resolution.** This is important in evaluating risk associated with open vulnerabilities.

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

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

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

The more qualitative evaluation, however, is whether the training actually changed people's behavior. You can try to figure that out by measuring a change in the volume of those kinds of calls to tech support, but is that change in call volume an indicator of successful training, or does it reflect an increase in those kinds of attacks? Executives want a quantifiable answer.

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

STEVEN PARKER

Senior Director,
Information Security
The Advisory Board Company

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

Website | Blog

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

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

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

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

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

KEY LESSONS

1. **A solid, standardized framework will answer many questions about how secure you are, but tracking the right metrics will drive your understanding deeper.**

2. **Your basic message to executives should be that secure systems are what make it possible to continue growing the business.**

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

- **Confidential records breached or stolen.** This metric gauges access control. The goal, of course, is to get the number of breaches down to zero through active personal information access auditing and monitoring. "What we want to show is that we have controls in place and are managing that access, regardless of who is coming into our environment," Parker says. "For me, access control is number one: you don't want to give away the keys to the kingdom."
- **Intrusion log audits.** These audits measure your understanding of which types of intrusion attempts are occurring within the security environment while also helping track time to resolution. "You want to make sure that your network team understands the intrusion attempt and is able to modify systems to defend against it," Parker explains. If network traffic usually occurs during business hours but there's a spike in accesses from China or Estonia at 3:00 a.m. on a Saturday, that should raise red flags. "It might be a minimal threat, it might not," Parker comments. "The key is how quickly you can detect it and respond to it. That's crucial."
- **Successful malware attempts.** This metric monitors the number of malware or phishing attempts that get past filters and that staff members click. This is the "people piece" that a lot of CISOs overlook, Parker contends. "People are going to make errors; they aren't infallible," Parker cautions. "Security awareness really plays a large role in reducing the number of successful phishing attempts." At Arise, he states, by monitoring this metric and fashioning an appropriate response, his team virtually eliminated successful email-based malware attacks in a little more than a year.

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

Parker thinks that the C suite's comprehension of information security matters is improving. It is nonetheless important, he says, to be selective and effective at communicating data that will matter most to the leadership team. They care about what security costs now and will cost going forward, Parker notes. "You want to be able to do these things without limiting the business," he states. Your metrics, then, should demonstrate to leadership that secure systems make it possible to continue growing the business. "It is important to get across to the C suite that they have a secure foundation and a good security program," he concludes. "You can grow the business knowing that those security bases are covered."

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