Mighty Guides

EMEA:

USING SECURITY METRICS TO DRIVE ACTION

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

Sponsored by:

tenable™

TABLE OF CONTENTS

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 cybersecurity program to your C-suite and Boards.

Amit Yoran
Chairman and Chief Executive Officer

tenable™

About Tenable

Tenable 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 U.S. 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. For more information, please visit tenable.com.

INTRODUCTION

As the challenge of securing digital assets grows, the challenge of quantifying an organization's security posture is also growing. This is due in part to the added layers of protection needed to secure IT infrastructures that have no perimeter, and the sheer quantities of data generated by new security technologies. It is further complicated, especially for global companies, by regional differences in security practices, standards, and regulatory environments.

In order to better understand how security organizations operating in Europe and the Middle East use metrics to describe their security posture, we decided to ask them. With Tenable's generous support, we posed this question to a number of security experts:

Your CEO calls you in and asks 'Just how secure are we?' What strategies and metrics would you use to answer that question?

For this e-book we spoke to a global audience, including people from Germany, France, the Middle East, and the UK. In these regions, security practices and regulatory environments are very mature. Yet politics often plays a role in which security frameworks can be used in certain countries. For example, a French company with global operations may use a US standard framework in its European operations, but it must adopt a different framework for its Middle East operations. Also, the risk landscape can vary considerably from one region to another, not only because of the nature of potential threats, but because of the varying costs of regulatory non-compliance.

Any business with operations in EMEA will find value in the perspectives of these EMEA-based security experts.

All the best,
David Rogelberg
Publisher

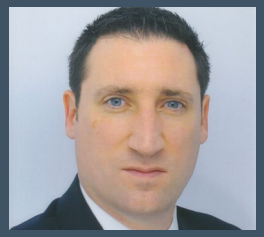
Mighty Guides

Mighty Guides make you stronger.

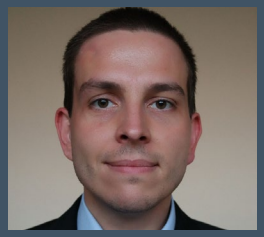
These authoritative and diverse guides provide a full view of a topic. They help you explore, compare, and contrast a variety of viewpoints so that you can determine what will work best for you. Reading a Mighty Guide is kind of like having your own team of experts. Each heartfelt and sincere piece of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



CÉDRIC THEVENET
DEPUTY GROUP IT INFRASTRUCTURE CISO AND ORM, SOCIÉTÉ GÉNÉRALE
Metrics Must Show That Security Expenditures Provide the Right Level of Protection
Pg 7



ARNAUD LAUDWEIN
CHIEF SECURITY & PRIVACY OFFICER, HACHETTE LIVRE
There's More to Security Metrics Than Raw Numbers
Pg 10

AANCHAL GUPTA
CISO, SKYPE MICROSOFT
With Security Metrics, Every Picture Tells a Story
Pg 14

SHAJU BHASKARAN
CISO, AHLIBANK QATAR
Metrics and Industry Comparisons Create a Complete Security Picture
Pg 17

ANDREW GREEN
CISO, APROSE RISK
Focus on Security Metrics That Demonstrate Cyber Resilience
Pg 20

We are vigilant in monitoring and enforcing that our security posture is being maintained as well as continuously looking for opportunities to improve our security stance. I would stay away from hard metrics e.g. Firewall block statistics and IPS metrics, and focus on a risk and risk mitigation based conversation as this is in line with the language that the board speaks.

Twitter

RICHARD TIMBOL

ISSM/CISO, Top 10 Global Law Firm

CÉDRIC THEVENET

Deputy Group IT Infrastructure CISO and ORM,
Société Générale

Cédric Thevenet has more than 15 years of experience as an IT security and operational risk management professional. He started his career working with a French intelligence agency and now works as a security consultant and CISO in major French companies.

Website | LinkedIn

Measuring the effectiveness of a security strategy is challenging for a large banking organization like Société Générale, which has multiple business lines and operates in 120 countries. It is important to make wise investment decisions in security, especially because no business has an unlimited security budget and it is never possible to eliminate risk completely. "Banks take risks all the time," says Cedric Thevenet, chief information security officer of Société Générale. "Our biggest challenge is defining where the risk is and how much risk we can tolerate."

Thevenet's security organization approaches this problem by using two teams:

- **One team focuses on external risk assessment and management.** This team collects information about emerging threats and new risks.
- **One team focuses on exposure, compliance, maturity, detection, and response.** This team evaluates the overall maturity of the organization's security posture in relation to other banks of similar size, assesses overall exposure based on several factors, and tracks compliance. "Compliance is critical," says Thevenet. "A bank that fails to conform to European compliance rules defined in the General Data Protection Regulation is subject to a penalty of 4 percent of its global yearly income. That's a big risk factor."

KEY LESSONS

1. **In considering which metrics best tell the bank's security story at an executive level, maturity statistics are among the most important.**
2. **For each business line, we evaluate the highest risks, our exposure to them, and their potential business impact.**

> *"Banks take risks all the time. Our biggest challenge is defining where the risk is and how much risk we can tolerate."*

In considering which metrics best tell the bank's security story at an executive level, Thevenet says that maturity statistics—that is, a measurement of security maturity relative to other banks of the same size—are among the most important. Maturity statistics take into consideration data from all aspects of the security operation. Thevenet says, "For each business line, we evaluate the highest risks, our exposure to them, and their potential business impact." Thevenet also looks at all the security projects to see how fully implemented they are as a measure of how effectively they are defending against various risk vectors. His teams also gather data from all the filings they must submit to regulatory agencies. "We use all that information to conduct self-assessment, but we also have an external assessment that gives us an objective view of how we are doing in relation to our peers," Thevenet says.

The maturity metric, which was developed internally at Société Générale, is on a scale of 0-4. "We consider 3.5 the optimum maturity level for us," Thevenet says. "If we go higher than that—to 3.6, 3.7, or higher—it means that we are spending too much money." The return on investment it takes to achieve those additional incremental risk reductions and security benefits is simply not worth the cost.

Thevenet points out that the industry as a whole is constantly improving security to address continuously changing threats. That means that his organization must also continuously improve its security just to maintain a 3.5 maturity rating relative to its peers. "We can reach 3.5 maturity level one year, but we know that we have to replace equipment, update our practices, and address emerging threats or our rating will decline. Our job of continuously improving security is never finished," says Thevenet.

That metric plays an important role in deciding how much money Thevenet's organization will have to spend on security. "Everything is decided in the context of what we need to do to reach that 3.5 metric each year," Thevenet says. "We look at the organization's ambitions, and then we build a strategy to reach that ambition. We consider all the risks and the threats, and we make a list of all the areas we have to cover. As we build the budget, we determine what is really important and how much it will cost, and then we decide on the best choices."

> *"We can reach a 3.5 maturity level one year, but we know that we have to address emerging threats or our rating will decline. Our job of continuously improving security is never finished."*

There is no 'simple' / one-size-fits-all method to answering "Just how secure are we?"—as in all things cyber 'it depends.'

–The security leadership must develop a 'CISO Scorecard' that assesses the many security/ risk measures that best embody a risk-based security strategy approach, distilling the many operational and strategic metrics into those that matter to the BoD.

–Any CISO scorecard is part art and science, whereas there is no shortage of authoritative sources on 'what' to measure; the art is then selecting those metrics that show both risk reduction and enhancing the business success and competitive advantage.

LinkedIn

MIKE DAVIS

Director, IT Security (CISO) at American Bureau of Shipping

THERE'S MORE TO SECURITY METRICS THAN RAW NUMBERS

ARNAUD LAUDWEIN

Chief Security & Privacy Officer,
Hachette Livre

Arnaud Laudwein is the chief security and privacy officer for Hachette Livre. Previously CISO for Meetic, the European leader in dating services, and PCI DSS project manager for Orange, he has extensive experience securing IT systems, including payment processing, and is a Project Management professional (PMP). He deploys strategies to keep customer data safe and bring actual security benefits to compliance projects. He uses security to simplify organizations and processes and help companies through their digital transformation.

Twitter | Website | LinkedIn

Arnaud Laudwein, chief security and privacy officer for Hachette Livre, says that "There are things that CEOs (chief executive officers) always comprehend—a percentage of progress, an explanation of the risk if we don't finish a project in time, and metrics that help them make decisions or prioritize over other business items." They need "metrics that show the effectiveness of security programs, but they do not always need to go into details—their usual question is 'Are we secure?' rather than 'How secure are we?'" Laudwein says.

KEY LESSONS

1. **Presenting a report filled with metrics to CEOs and executives doesn't provide an understandable picture of security. They need context to understand how the metrics translate to business objectives.**

2. **Meeting compliance requirements doesn't mean that nothing else needs to be done. Standards cannot take into account the specificities and potential weaknesses of each business.**

Present Metrics in Percentages

"Just throwing a big report at the CEO or C-level executives will not help them much," he says. "We calculate technical metrics like the percentages of servers that are up to date and how quickly we patched them. These day-to-day metrics show that we are aligned with our goals." Laudwein says that simply presenting those numbers to the C-suite will complicate the question of how safe the organization is, however. "A CEO does not always need all the detailed metrics. We should have them for ourselves, but C-suite executives want to know if the results are good or not, and how we plan to improve them."

> *"There are things that CEOs always comprehend—a percentage of progress, an explanation of the risk if we don't finish a project in time, and metrics that help them make decisions."*

THERE'S MORE TO SECURITY METRICS THAN RAW NUMBERS

To accomplish putting technical metrics into terms that are important to executives, Laudwein suggests focusing on metrics associated with projects that make the company more secure. "It's not a metrics presentation," he says. "It's showing which projects we will be working on and how they help make the company more secure." He says, "We try to show progress as percentages, not raw numbers." Rather than telling that 200 servers have been patched, explain that 5 percent of the servers have been patched, which means that 95 percent are still vulnerable.

Alternatively, Laudwein says, "Analyze the percentage." In other words, provide some context that relates to the prioritization of critical and vulnerable assets for the metrics you provide. For example, he says "maybe we patched only one server, but it was the server that contained all the mission-critical company data. Show progress on a project or metrics that will help the CEO make a decision."

Don't Rely on Compliance Metrics

One thing Laudwein warns against is relying solely on compliance metrics. "It's nice to say that we are compliant, and in some cases it's an obligation," he says. "But for the CEO, too often it means, 'Oh, it's good. Nothing else needs to be done because we received our certification.'"

Laudwein notes, "A lot of compliant companies have been hacked." Target Corporation is a good example; Laudwein says that Target even went as far as to have an external, onsite audit and was still breached. Laudwein suggests that is because, "Each company is different, and the standards cannot take into account the specificities and potential weaknesses of each business. Having a compliance requirement helps having the required budgets, but compliance metrics alone are not a good indicator of how secure a company is."

> *"In addition to the technical metrics, we focus on nontechnical metrics such as how aware our teams are or how secure our partners and our business processes are."*

Consider Nontechnical Metrics, Too

Finally, Laudwein says that technical metrics are not the only method of illustrating how secure an organization is. "In addition to the technical metrics, we focus on nontechnical metrics such as how aware our teams are or how secure our partners and our business processes are." For example, Laudwein says, "A lot of security breaches come from third-party vendors that were breached."

Nontechnical metrics, he says, are "anything that can allow hackers to enter your network or gain information about your network." The nontechnical metrics work together with technical metrics and percentages or project-focused metrics to help create a complete picture of just how secure an organization is.

Based on our organizational risk appetite, and our own risk analysis, we are as secure as we can be within our budget, people and organisational constraints. We have addressed the top 10 most harmful cyber risks to the business using a mixture of approaches, are continuing to monitor those top 10 risks and approaches, and have rehearsed plans to help us deal with new or unexpected risks.

Twitter I Website I LinkedIn

ADRIAN DAVIS

Managing Director EMEA, (ISC)²

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 | LinkedIn

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."

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.**

> *"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?'"*

- **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?'"

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."

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

If you're tracking metrics for things that aren't tied to what you're trying to achieve, you're failing. And if you're tracking metrics for things that you have no intention of ever acting on, you're also failing. The primary questions should be, 'why am I tracking this, and what do I intend to do when I get a certain result?'

Twitter | Website | Blog | LinkedIn

DANIEL MIESSLER

Director of Advisory Services, IOActive

SHAJU BHASKARAN
CISO,
AhliBank Qatar

Shaju Bhaskaran has 16 years of experience in information security, cybersecurity, risk management, compliance and audit, IT security, and business continuity management and disaster recovery consulting. He gained this experience while working for such global organizations as Standard Chartered, General Electric, ING, and Dimension Data. Shaju holds CISSP and CISA certifications.

Twitter | LinkedIn

Shaju Bhaskaran, chief information security officer (CISO) of Ahli Bank QSC, says that illustrating a level of security for the chief executive officer (CEO) is a matter of knowing which metrics to share and how to share them. "Every organization has its own appetite for risk and an acceptable level of security. A bank would have more security in a specific region; a different company in another region may have a different level of security. So, the level of security and the controls implemented depend on marketable factors." Bhaskaran says, however, that you should not disclose all the metrics you track, regardless of the requirements of your region. "You cannot communicate all the alerts and all the metrics that you may have readily available" because so much information is impossible to explain in a way a CEO can understand.

Bhaskaran explains, "In security, there may be certain controls that you implement in your organization—maybe 15 or 20 different controls, of which perhaps 75 percent would be operational in nature, such as your antivirus solution, your Internet security tools, access-related issues, incidents, day-to-day email, and web security–related issues. If you know your threshold for risk and the value of each metric, then you can respond accordingly." The problem with these metrics, says Bhaskaran, is that they do not really illustrate security. "I would focus more on the perimeter defense and critical alerts, which are more about the time to exploit that attack into a major incident."

KEY LESSONS

1. **Focusing on operational metrics may allow you to present impressive numbers, but it will do nothing to tell the CEO just how secure the organization is, so it's important to focus on critical metrics that have deeper meaning.**

2. **When communicating security levels to the CEO, focus on a comparison with other companies within your industry and your region as a way to illustrate security levels and your ability to resist or respond to attacks that have created issues with those other companies.**

> *"Every organization has its own appetite for risk and an acceptable level of security."*

Those, Bhaskaran points out, "might be certain metrics that are more critical in nature, depending on the region and the industry. For example, we are prone to distributed denial of service (DDoS) attacks. DDoS attacks would be critical in nature." Bhaskaran says he also considers Domain Name System (DNS)–related attacks, new malware alerts, advanced persistent threats (APTs), and intrusion-prevention system (IPS) alerts critical metrics that should be communicated to the CEO. "These are the primary metrics I would focus on," he says. These metrics help him apprise the CEO of the most critical security risks—the risks that need the most attention. By contrast, Bhaskaran says, metrics he would avoid include "access-related issues, something related to a normal antivirus alert, or something related to email, web security, or database alerts. If it is operational in nature and within the threshold, I would not communicate this detail to the CEO."

To ensure that the CEO understands the metrics, Bhaskaran suggests that, "The metrics shared should correlate with some reference that you should have for the industry and the region. We get constant information about attacks that have happened in the region or within the industry." For example, in the banking industry, Bhaskaran says, "We can relate those metrics to the issues that we see in other banks. Our metrics should clearly define the status of our controls with respect to the industry and the region."

"The risk appetite of your organization should be your primary focus. The level of controls that you build for your IT infrastructure should always indicate what the organization has with respect to similar size organizations in your industry rather than comparing them with every type of organization." Using this technique, Bhaskaran says not only can you keep your organization safe, but you can clearly communicate with the CEO just how secure the company is.

> *"If you know your threshold for risk and the value of each metric, then you can respond accordingly."*

At the present time there are no major, ongoing, security incidents being reported. Several measures are in place to prevent and detect incidents in the shortest amount of time possible when a breach occurs, and the appropriate response plans have been put in place based on the sensitivity of the data on the affected systems and the importance to business operations.

Twitter | Website | LinkedIn

PAUL ASADOORIAN

Founder & CEO, Security Weekly

FOCUS ON SECURITY METRICS THAT DEMONSTRATE CYBER RESILIENCE

ANDREW GREEN

CIO,
Aprose Risk

Andrew Green is chief information security officer and co-founder of Aprose Risk; a London-based, independent consultancy that specializes in solving organizations' cybersecurity challenges. For the past 15 years, he has worked internationally for clients in financial services, government, and defense. He has a master's degree in Information Security Management, is a certified CISSP, CISM and is a Fellow of the British Computer Society.

Twitter | Website | LinkedIn

"When working with clients to address their cyber challenges, we focus not on cybersecurity but rather on cyber resilience," says Andrew Green, chief information security officer (CISO) of Aprose Risk.

"It has become a truism that every organization will suffer a security breach, and consequently organizations need to consider how quickly they're able to respond to, and recover from the breach," Green says. "This focus on response and recovery is at the core of cyber resilience, and the metrics that measure this are essential to an effective program. To have a resilient organization, a holistic and systemic approach is needed. You need to consider not only the technology, the people and the processes, but also the protective, detective, and responsive controls for each of these," he explains.

KEY LESSONS

1. **Moving towards greater sharing of metrics is key for the collective attack surface to be reduced.**
2. **Frame security metrics in a meaningful, understandable context to ensure that CEOs and other executives understand not only the risks the organization faces but also the strategies needed to achieve security.**

"In practice, most organizations are spending around eighty-five percent of their security budgets on protective, technical controls. They are putting very limited expenditure towards detective and responsive controls, and very little focus on the people and the process aspects of cyber resilience," Green says. "Strong metrics can highlight these areas where greater focus or maturity are required".

> *"We are advising organizations on how to become more resilient, and which metrics are key in understanding if their cyber capabilities are mature enough."*

"In addition, the metrics should be built around those controls and be meaningful," continues Green. "The sorts of metrics we often see for protective controls are highly technical such as 'port scan frequency' or attempts to get through the firewall. For detective controls, we see events in log files which can be difficult to interpret. These numbers alone don't tell a compelling story," says Green.

"For example, a key control in developing robust resilience is 'ethical phishing,' whereby the organization sends benign phishing emails that mimic real-world threats to demonstrate how susceptible they are. When we then report back to them that say 60 percent of the organization is susceptible to a phishing email, they realize the threat that they are facing. This is where I see chief executive officers (CEOs) really take an interest, become engaged, and lean forward to hear more," he says. "It brings security to life because the CEO understands phishing emails; they receive them themselves, both at work and at home. It is contextualized for them and has business impact relevance."

Green also strongly believes that organizations need to compare metrics across the industry. "What we're often asked to explain to the CEO or the board is, 'are we secure compared with our peers?' And I think that's valuable." In fact, requirements in the United Kingdom are maturing to support this sharing of information. "Here in the UK, the Cybersecurity Information Sharing Partnership (CISP) is a relatively new approach whereby organizations are encouraged to share their metrics so that they can benchmark and make sure that their approach is appropriate for their industry and the risks that they're facing. These sharing initiatives need to develop further and organizations should consider a more altruistic approach. Everybody is concerned about their own well-being but not necessarily about the well-being of the community. That cultural change needs to happen." Comparing company metrics with the industry also helps to provide context for the CEO or C-suite.

"In summary, we are advising organizations on how to become more resilient, and which metrics are key in understanding if their cyber capabilities are mature enough. It includes the areas of technology, people and process, and protective, detective and responsive controls. The metrics used need to be meaningful in order for decisions to be made from them, and moving forwards greater sharing of metrics is key for the collective attack surface to be reduced."

"In the UK, the Cybersecurity Information Sharing Partnership (CISP) is a relatively new approach whereby organizations are encouraged to share their metrics so that they can benchmark and make sure that their approach is appropriate for their industry and the risks that they're facing."

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…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.

LinkedIn

NIKK GILBERT

Director of Global Information Protection and Assurance, ConocoPhillips

SECURITY METRICS THAT TELL A STORY TO THE BOARD

ISTVAN RABAI
CISO,
SIGNALHORN TRUSTED NETWORKS GMBH
Security Metrics Are About People and Money
Pg 25

KYLE HASTINGS
DIRECTOR, CYBER RISK SERVICES,
ONE OF THE BIG 4 CONSULTING FIRMS
Communicating Security Requires Two Vocabularies
Pg 28

DARYL FLACK
CIO,
BLOCKPHISH
Foundational Metrics Help Build a Security Narrative
Pg 31

IRENE CORPUZ
HEAD OF PLANNING AND IT SECURITY,
ABU DHABI GOVERNMENT ENTITY
When Reporting Security Initiatives to Management, Keep It Simple
Pg 34

AARON WELLER
MANAGING DIRECTOR,
CYBERSECURITY & PRIVACY
PRICEWATERHOUSECOOPERS
The Best Security Metrics Are Actionable
Pg 37

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

Twitter | Website

ROBIN "MONTANA" WILLIAMS

Senior Manager, Cybersecurity Practices & Cyber Evangelist, ISACA

SECURITY METRICS ARE ABOUT PEOPLE AND MONEY

ISTVAN RABAI
CISO,
Signalhorn Trusted Networks GmbH

Istvan Rabai, CCNP, CEH, ECSA, RHCSA, CISSP, began his career as a systems engineer, programming IBM AS/400 computers and building fiber-optic token ring networks. Since 2010, he has been working for telecom company Signalhorn in Germany as manager of IP Networks. In February 2016, he took on the role of CISO, managing the PCI DSS– and ISO 27001–compliant security operations for Signalhorn.

LinkedIn

When Istvan Rabai came to Signalhorn, security had not previously been an area of focus. As a result, he had a lot to do to harden the company network and secure corporate digital assets. To overcome the awareness challenges, Rabai needed to determine how best to frame the importance of security in a language that the C-suite would understand. "The CISO (chief information security officer) might be interested in technical measures—say, the number and priority of relevant vulnerabilities or the number of infected PCs," he says. "For a CEO (chief executive officer), these numbers do not mean anything. The CEO wants to see how much return on investment he or she will get."

KEY LESSONS

1. **If you want the CEO to understand the importance of security investments, frame the message in a language he or she understands, by providing metrics, real-world examples, and monetary results.**
2. **Educating both senior management and network users on the threats the network faces is one of the most efficient ways to ensure their cooperation in protecting the network.**

To illustrate this point, Rabai says that he uses a combination of metrics and a story, either from the company's past or from another company, to highlight the risks of not being properly secured. "I present our current security posture by showing that we haven't had any major security breaches, and we have had no money loss since we hardened the core network." For example, Rabai may present the CEO with the number of intrusion attempts, and then share a story about how another company was breached, with the monetary losses that company experienced. "Senior management's language is money," he says. "This is why a CISO needs to speak money. The CEO or president of a company rarely understands technical terms."

> *"I present our current security posture by showing that we haven't had any major security breaches, and we have had no money loss since we hardened the core network."*

SECURITY METRICS ARE ABOUT PEOPLE AND MONEY

In addition, Rabai made security awareness training a priority. “This is what keeps me awake at night. The Payment Card Industry Data Security Standard requires that we conduct security awareness training yearly. Instead, I do it every two months.” The result, he says, is that network users now understand the “why” of security control.

For example, he used awareness training to enlighten users on the risks of phishing attacks and how to avoid being compromised. As a result, when a senior manager received an email that looked like it came from the CEO requesting that a large amount of money be transferred to another account, “the senior manager recognized the signs of the fake email,” Rabai says. “He checked with the CEO and did not respond to the attacker.”

“In contrast, the employees of another company received a similar email,” he explains. “They did not recognize that this was a fake email and transferred a huge amount of money to the attacker’s bank account. When our senior management got this news, they realized the importance of the training we do here in the security field every day. This is how it gets to them—through money.”

Rabai says he used this example to demonstrate just how valuable and practical the company’s security investments are. “I make what we are doing here real for them,” he says.

> *“Senior management’s language is money. This is why a CISO needs to speak money.”*

You need to have metrics and messages across security that are specific, measurable, attainable, relevant, and time-bound. If you don't, you are going to lose your audience.

OMKHAR ARASARATNAM

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

COMMUNICATING SECURITY REQUIRES TWO VOCABULARIES

KYLE HASTINGS

Director, Cyber Risk Services,
One of the Big 4 consulting firms

Kyle Hastings is a director at one of the Big 4 consulting firms, where he advises global financial services clients on how best to manage the cyber risks that arise from their business activities. Prior to joining that firm, Kyle was global CISO at VTB Capital; before that, he spent six years at Barclays, last serving as the global head of Technology Risk for Barclays Wealth and Investment Management. Kyle started his career as a cryptologic officer in the U.S. Navy.

LinkedIn

"When are metrics useful? When you're running your IT security operationally," says Kyle Hastings, a director of Cyber Risk Services for a global consulting firm. "You have to do the basics right and it's very important to know how you are doing on patching your servers and workstations, and where you are with your antivirus updates and endpoint protection. Your incident response and security operations teams need to know, are they getting more efficient at closing off incidents? Are their response times getting faster? The length of time threats persist in the enterprise—is that getting shorter? These metrics are useful operationally for understanding how well your IT security teams are doing their jobs, but I don't find them particularly useful at the board or chief executive level because they're quite technical and low-level. Board members generally don't speak technology, but they do understand risk, so you have to have two different vocabularies to communicate effectively."

KEY LESSONS

1. **Ask the C-suite or the board what their top management concerns are to understand what the business's risks are. Then you need to examine if they are comfortable with the risk levels in these top areas of concern.**

2. **Making metrics meaningful to the CEO or the board comes down to the way you talk about security. Save the technical metrics for managing security operations, and speak to the risk the organization faces.**

The question is, how do you determine which risks are most important to the C-suite or board? Hastings suggests that the best way to determine the top management concerns is to simply ask them. "They're not my risks; they're the business's risks. They are where the business leaders think they see problems. You can do it solely top down," he says, "but I think it also helps to do it bottom up and meet in the middle."

> *"Board members generally don't speak technology, but they do understand risk, so you have to have two different vocabularies to communicate effectively."*

COMMUNICATING SECURITY REQUIRES TWO VOCABULARIES

What Hastings means is that it can be useful to present the board with some of the risks you see as the person in charge of security. "By doing it from the bottom up, you can go to the C-suite with points to help get them thinking, but you don't want to dictate the risks to them; You want *them* to tell you what keeps them up at night."

When you know the C-suite or board's worries, you can begin to examine whether you have the controls in place to protect against those risks. With a clear view of what you have, you can identify the residual risk left by gaps in coverage. "Then, you take that to the C-suite and say, 'This is the residual risk we're running in your top areas of concern. Are you comfortable with this? Is this above or below your risk appetite?'"

The responses to those questions open the door to implementing better security controls. "If the response is that the residual risk is above risk appetite, you're likely to need a program or project to mitigate that risk. That's going to cost money. The true expression of risk appetite is budget. If they're not willing to give you money, then they're not really worried about it," Hastings says. "If they give you money, there's a genuine concern."

"Obviously, security is an iterative process. You don't just do it once and stop. You'll revisit those risks every year. You'll ask, 'How has the threat landscape changed? Do we have new risks now? Have we started new lines of business? Have those new lines introduced new risks to the organization?'" Hastings says that if he doesn't have the right framework in place to answer these questions, then any answer he might give a chief executive officer (CEO) about security or risk appetite would be meaningless.

"There is no way you can answer the security question simply with metrics because security is relative," he adds. "How secure are we compared to what? Using the top risks that face the organization and where we are with respect to the organization's appetite for those risks removes the relativity as you're measuring against a standard you've set for yourself." Ultimately, Hastings says, making metrics meaningful to the CEO or the board comes down to the way you talk about security. "You have to pick the right vocabulary to communicate with the audience effectively."

> *"The true expression of risk appetite is budget. If they're not willing to give you money, then they're not really worried about it."*

By comparing your assets, controls, and vulnerabilities, you are able to have a better view of your security posture. And with that visibility, you can make the decisions you need to make, such as what you're willing to spend to align your security posture to your risk appetite.

Twitter

TROELS OERTING

Group Chief Information Security Officer, Barclays

FOUNDATIONAL METRICS HELP BUILD A SECURITY NARRATIVE

DARYL FLACK
CIO,
BLOCKPHISH

Daryl Flack has 16 years of experience delivering secure technology solutions and business transformation. He has worked internationally in a variety of sectors, including digital media, retail, legal, construction, central government, and defense. In addition to his role as CIO of BLOCKPHISH, an ethical phishing and cyber-awareness learning company, Daryl provides security guidance to government and industry on the Smart Metering Programme, which aims to roll out 53 million smart meters in Great Britain by 2020.

Twitter | Website | Blog | LinkedIn

"Security culture starts at the board and flows down to the organization's employees," says Daryl Flack, chief information officer (CIO) of BLOCKPHISH. "To provide value, you must understand what metrics are required to support your business objectives."

Flack recommends, "Concentrate on the fact that you're there as an enabler, and everything you do is there to help the organization be better at what it does, whether that is helping to communicate and drive performance, measure effectiveness or to support decision making. It's important to make cybersecurity a differentiator, because when you align it with the core of what you do in business, it then becomes a powerful enabler to make the business more successful and resilient."

"Security metrics are helpful in this as they support the ability to tell a story," he says, "but it's the narrative that goes with the metrics and the strategy that goes around it that helps people visualize how you're performing as an organization."

KEY LESSONS

1. **Metrics are useful tools for viewing a snapshot of security, but those metrics are meaningless unless a relevant and understandable narrative go with them.**

2. **Achieving compliance doesn't necessarily mean that your organization is secure. Communicating the intent of the compliancy requirements to your staff and ensuring they understand their importance will help make you more resilient.**

> *"Security metrics support the ability to tell a story, but it's the narrative that goes with the metrics and the strategy that goes around it that helps people visualize how you're performing as an organization."*

FOUNDATIONAL METRICS HELP BUILD A SECURITY NARRATIVE

"The specifics of which metrics are most important depend on the organization," states Flack, but he also points to a few metrics that are universal for organizations. For example, he says that since phishing accounts for an estimated 91% of all cyber breaches, the number of phishing attempts, the number of times users click phishing links, or the number of times users report phishing emails are all good baseline statistics, as they measure the performance of people, process, and technology.

Flack continues, "It's always good to have the traditional transactional statistics such as how many security incidents and events are logged and managed." However, he explains, "It's one thing to have a snapshot of where you are, but the real value comes in the trend analysis of tracking whether you're improving on that metric or declining, and what you should be doing about it."

Flack also warns not to rely too heavily on compliance regulations as a means of communicating security. "Compliance will help you pass an audit, but it won't necessarily mean that your organization is secure. Many leading organizations that recently suffered security breaches were all compliant with their relevant certifications. It's how you communicate the intent of those compliancy requirements to your staff and how well they understand the importance of them to their role that will help make you more resilient." Providing all staff with long, wordy policies and then blaming them if they don't follow them is not helpful for either party.

Statistics and policies don't mean anything unless you've got an ongoing security awareness program for your staff to help them understand and support your security objectives. Security is not just about having a snapshot of your current state or a once-a-year compliance tick box exercise. It's something that needs to be embedded in your culture and live throughout the whole organization all the time.

There are a wide variety of technical security metrics and statistics you can generate and measure, which can all provide value. However, you must align metrics, embed cybersecurity culture within the organization, and constantly measure effectiveness in order to ensure that you're providing your organization with the right measurements and statistics required to promote and improve cybersecurity resilience.

> *"It's one thing to have a snapshot of where you are, but the real value comes in the trend analysis of tracking whether you're improving on that metric or declining, and what you should be doing about it."*

You can select at most five metrics that are both qualitative and quantitative, and each [executive team] individual will pick up something he or she understands.

LinkedIn

GENADY VISHNEVETSKY

CISO, Stewart Title Guarantee

WHEN REPORTING SECURITY INITIATIVES TO MANAGEMENT, KEEP IT SIMPLE

IRENE CORPUZ

Head of Planning and IT Security,
Abu Dhabi Government Entity

Irene Corpuz has 26 years of diversified experience in IT, including IT service management, strategy, risk management, and information security. She is currently responsible for the implementation of the United Arab Emirates National Electronic Security Authority Information Assurance Standards (IAS) in an Abu Dhabi government entity. She also contributes her skills and expertise in information and cybersecurity through conferences, blogs, and articles. Corpuz holds several certifications and has received local and international awards.

Twitter | LinkedIn

In her role managing security and other network functions for a large government entity in Abu Dhabi, Irene Corpuz has learned that, when it comes to reporting up, "keep it simple." This means when preparing a report for the general manager, for example, she keeps the presentation to four pages, which she feels are already too many. "The first page is a title," she says, "the second page is what is expected of the report, and the third and fourth pages are the main reports." These reports focus heavily on two areas: risk level and governance.

"They will not listen to you if it is more complex than that," says Corpuz. So when she sends her reports with a note saying, "for your information, sir, this is just a two-page report. Then he will open it," she says. "If you don't say that, they will not even click on the attachment."

But that level of simplicity in reporting is only for executive management. In Abu Dhabi, the Abu Dhabi Systems and Information Center mandate specific standards or requirements on all government entities. For government agencies focused on law enforcement or those where a data breach would be potentially catastrophic, the highest level of security compliance is reported. The National Electronic Security Authority (NESA) collects the data and is the government body tasked with protecting the United Arab Emirates' critical information infrastructure and improving national cybersecurity.

> *"To some, they hate measures, but to people who understand why measures are important, they will value why we are doing this. This is our tool to justify a budget."*

KEY LESSONS

1. **Reporting to a government agency is more complex than to a CEO or director, who typically prefer less technical analysis.**
2. **Training and awareness among the team are just as important as compliance.**

So for Corpuz, meeting NESA requirements is a minimum starting point in defining security effectiveness. Although her reporting to internal management within the government agency is fairly simple and in layman's terms, for NESA, she completes a much more thorough and templated report. "When [NESA] are collecting various reports from all government entities," Corpuz says, "they should be reading the same type of report; otherwise, it will be difficult for them to consolidate and understand the reports if we have our own way of reporting."

Compliance is only part of the battle, though, according to Corpuz. The most effective security practices begin with awareness and training, she says, as it is difficult to assess risk without knowledge of both the data being protected and the governance processes in place at each organization.

And while most organizations place a strong emphasis on business continuity and damage control should there be a breach, Corpuz suggests that reputation must also be a prime consideration. "During the gap analysis or risk assessment," she says, "we determine the impact of the information that we are keeping as a government entity when there are data breaches." Here is where metrics play a big part, says Corpuz. "To some, they hate measures, but to people who understand why measures are important, they will value why we are doing this. This is our tool to justify a budget, to say why we need this, and metrics are our way of presenting the return on investment for each specific solution that we implemented, including training and recruitment."

> *"Metrics are our way of presenting the return on investment for each specific solution that we implemented, including training and recruitment."*

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

Twitter | Website | Blog

ED ADAMS

CEO, Security Innovation, Inc.

THE BEST SECURITY METRICS ARE ACTIONABLE

AARON WELLER

Managing Director, Cybersecurity & Privacy, PricewaterhouseCoopers

Aaron Weller is a managing director in PricewaterhouseCooper's (PwC) Cybersecurity & Privacy practice, with responsibility for leading this practice for the US Pacific Northwest. He has more than 18 years of global consulting and industry experience, including several years each in Europe, Australia, and the United States. Prior to joining PwC, Aaron co-founded and ran an information security and privacy strategy consulting firm and held such roles as chief information security and privacy officer for two multinational retailers.

Twitter | Website

In many ways, corporate data security is fundamentally a resource allocation issue. "There's never enough time, there's never enough money, and there's never enough people, so allocating the right dollars to protecting the most sensitive types of data is the central challenge," says Aaron Weller. To win the necessary resources, you need to align essential security goals to strategic business objectives; then, you must achieve these goals in a way that meets expectations.

An important part of accomplishing this is using the right security metrics to show what has been done and what needs to be done. But what are the metrics that resonate with board members and C-level executives? To begin with, you must use metrics that drive the right kinds of decisions and behaviors. "A good rule of thumb," explains Weller, "is that if a metric changes and you wouldn't change your activities as a result, it's a bad metric." So, for example, you might report that you blocked 500,000 attacks on the firewall last month. That's great, but what if it was 600,000 or 400,000? Would you do anything differently? If the answer is no, there's no point in reporting that metric until it hits a trigger value when the behavior would change in response.

KEY LESSONS

1. **Activity metrics are useful only to prove that you're doing something, but they don't show how effective that activity is.**
2. **Everything that gets presented to the board has to have a clear link back to business value and business strategy.**

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

THE BEST SECURITY METRICS ARE ACTIONABLE

Weller describes three tiers of security metrics:

- **Activity metrics.** These simply provide a measure of how many times we do something or how many times an event occurs. Examples include how many vendor reviews we've done or a metric that says we doubled the number of vendor reviews in the past year. "Activity metrics can appear to be interesting," says Weller, "but they rarely if ever give us information that drives actions or behaviors. They are useful only to prove that you're doing something, but they don't show how effective or efficient that activity is."
- **Trend metrics.** Trend metrics are more informative: they can provide insight into the effectiveness of a security program. For example, if we identify 10 percent of the vendors we review as high-risk vendors, look at the average time between reviews for those vendors, then look at how that number trends, we have a metric that can be related more specifically to a particular business outcome, in this situation whether the highest risk vendors are being assessed on a cadence that is aligned with the organization's appetite for risk.
- **Outcome metrics.** "Outcome metrics are the ones that really matter to the board," says Weller. For example, an outcome metric might show how our actions actually improved the vendor-management process by eliminating risky vendors in a way that has enabled us to more effectively reach our strategic goals. Weller explains that "outcome metrics speak to the value of the activities you're performing. The executive audience is significantly more interested in the outcome than the activity itself."

Many tools are great at producing metrics, but most of those metrics are activity based. "A lot of metrics presented to the board are backwards-looking activity and trending metrics," says Weller. "What's really needed is outcome metrics and forward-looking trending metrics that indicate where we plan to be next year, which can be supported with a story on what actions will be taken to get there. That becomes the basis for decisions that shape the security program moving forward." Yet Weller says that in his experience, not enough of this kind of metric data is presented to the board in many companies. Everything that gets presented to the board has to have a clear link back to business value and business strategy.

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

It is important to raise issues using a risk-based language that allows the board to make risk-based decisions on cyber-security spending.

Twitter | Website | LinkedIn

SCOTT SINGER

CISO, PaR Systems, Inc.

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. For more information, contact us at:

EMEA Headquarters
Tenable Network Security
81b Campshires
Sir John Rogerson's Quay
Dublin 2, Ireland

Germany
Tenable Network Security
Prielmayerstraße 3
80335 München
Deutschland
+0049 (0)221-8282-9194

London
Tenable Network Security
3 Furzeground Way
Stockley Park, Uxbridge
Middlesex, UB11 1EZ
United Kingdom
+44 (0) 330 808 4684

Find more thought leadership information at: CISO Resources

Learn more about how other organizations are using Tenable solutions: Case Studies