Mighty Guides

Sponsored by

NEHEMIAH SECURITY

7 Experts on Justifying Security Spend

Prioritizing Security Needs to Senior Management and the Board

INTRODUCTION

When it comes to cybersecurity, every organization builds a program based on its own asset portfolio, unique business culture, and operational challenges. Regardless of its specific needs, every security program must do two things: prioritize, and sell itself to senior management. How do security executives do this successfully?

With generous support from Nehemiah Security, we asked seven security experts the following questions:

How would you advise a new CISO in justifying their prioritization and spend to senior executives, and what strategies would you recommend for communicating needs and risks to management?

In speaking with security practitioners from diverse industries, it is clear that the key lies in how they quantify the business impact of risk. However, risk means different things to different businesses. The challenge then comes down to deciding what is most important to the business, what are the true costs of losing it, and how that compares to the cost of preventing its loss.

The essays in this eBook offer practical strategies, advice, and examples showing different approaches to calculating risk, and how to use that effectively in presenting to senior management. I'm certain anyone who needs to justify their security program will benefit from the experiences of these professionals.

All the best,
David Rogelberg
Editor

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.

FOREWORD

I speak with security and business leaders every week. They all have one thing in common. They all want to know what their biggest risks are, and what they can do to lessen those risks. For most of the business—finance, people, competition—controlling risks is a well-defined science. This is not the case for cybersecurity.

We created this Mighty Guide to advance the risk management conversation amongst cyber professionals. Many would claim they are able to pinpoint technical cyber risks. Few would profess a high level of confidence that they always deploy their resources to the biggest risks facing the company. Fewer still would say they effectively communicate this to their board.

We decided to make this personal by posing the question, "What would you tell your friend who just took over as CISO…?" This forced the respondents to be invested in a successful outcome. We were pleased to learn a few things: 1) cyber leaders recognize cyber risk as a real challenge, 2) the road to managing cyber risk effectively is actually a journey, 3) even the most progressive companies are finding themselves at the very beginning of this journey.

The conversations in this eBook will change the way you manage cyber risk within your business.

Regards,

Paul Farrell

CEO, Nehemiah Security

LinkedIn

NEHEMIAH SECURITY

Nehemiah Security delivers a cyber risk analytics solution that empowers the alignment of business and security. We believe security risk should be integrated into the suite of risks faced by businesses. The security conversation must evolve to answer the question 'Where is the best place for my next cyber investment?' We work with clients to quantify their technical risks in dollars and cents with the mission to facilitate communication with the C-Suite and justify cyber spend. CISOs that embrace this journey act with the confidence they are not only securing their systems but also operating within the best interests of the business.

NEHEMIAH SECURITY

nehemiahsecurity.com

Cyber Risk Analytics: Where do you **stand?** Where do you **start?**

Download the FREE Buyer's Guide

DOWNLOAD NOW

TABLE OF CONTENTS

TO QUANTIFY RISK, ASSESS POTENTIAL LOSS EVENTS

VICKY AMES

Director, Information Security
Marriott International

Vicky Ames has worked in the information security industry for 20 years. As director of information security at Marriott International, she is responsible for the strategic direction and management of the organization's risk and vulnerability management programs. Her experience includes building and leading security programs for the federal government as well as in the private sector, owning a security startup, and serving as president and CEO of a security consulting firm. She is a published author and frequent speaker on security and risk topics.

Twitter I Website

As an accomplished information-security professional with more than 17 years of experience in the field, Vicky Ames believes that it's important for chief information security officers (CISOs) to make sure that they understand the business, how it operates, and its regulatory environment. "Security should be the group that is enabling business, and you can't enable a business until you understand the nature of that business," she explains. "So understand your revenue streams and understand what is critical up at that level so you can tie that back to what you can deliver. That way, you understand what will be most important from an organizational risk perspective."

Ames also advises engaging an independent consultant to conduct a maturity assessment early on. "You need to get a dispassionate third party's view of where you truly are and what the status is when you're walking in the door," she says. From there, you can use that information to start building your security program and your road map. Armed with this insight, you can engage with leadership on specific strategies you want to pursue.

Ames and her team have begun using both a top-down and bottom-up approach to assessing risk in their environment in which they talk to executives to figure out what they're concerned about, then look more tactically below to understand the potential "loss events" of greatest concern. "When I say loss event, I'm talking about a monetary loss, or a cost incurred, for the company. That's ultimately what business leaders care about. We security professionals get very excited by the latest outbreak that's going on, but what the executives really need to understand is, 'What's my dollar exposure here?'" she notes.

> *"Security should be the group that is enabling business, and you can't enable a business until you understand the nature of that business"*

TO QUANTIFY RISK, ASSESS POTENTIAL LOSS EVENTS

To answer this question, Ames uses a method called the factor analysis of information risk. "This risk-assessment methodology helps you to quantify your risks and put them into dollar terms," she says. As part of the process, you can perform several analyses that roll up to a very large risk. For example, a very large risk might be antiquated Windows systems, in which case you would talk to people to learn more about the potential loss events associated with that risk. When determining what concerns them the most about those antiquated systems, you might find that some contain sensitive data while others run critical business processes which result in different loss events that need to be examined.

"You want to examine costs associated with each loss event to truly understand what the dollar loss could be to the company," Ames says. "So, the factor analysis of information risk is a structured methodology. It's one of the first ones to specifically target IT security and do that kind of quantification." This helps businesses overcome the communication challenges that often arise when IT security people talk about risk in technology terms and business people want to hear about risk in business terms. In those cases, she says, "The bridge is money."

When having conversations about risk management, Ames and her

> "We security professionals get very excited by the latest outbreak that's going on, but what the executives really need to understand is, 'What's my dollar exposure here?'"

colleagues come up with a potential loss figure associated with a particular risk. "Then we will go back and we'll say that if we purchased this tool or if we get this person and they do these things and it reduces the risk, we think that we can spend $10,000 to mitigate $4,000,000 in potential loss down the road," she says. This way, executives can make an informed decision about security investments that more accurately reflects the risks the business faces. ■

KEY POINTS

1 **A risk assessment methodology that analyzes loss events in terms of dollar amounts can help quantify the risks a business faces.**

2 **Dollar figures provide a common point of reference for security professionals and executives when conducting risk assessments.**

YOU MUST RELATE REQUESTS TO CONCRETE PROBLEMS YOU WILL SOLVE

RICHARD RUSHING

CISO
Motorola Mobility

As CISO for Motorola Mobility, LLC, Richard Rushing participates in corporate, community, private, and government security councils and working groups setting standards, policies, and solutions to security issues. He has put together an international team to tackle the emerging threats of mobile devices, targeted attacks, and cyber crime. He has developed and deployed practices and tools to protect intellectual property across the worldwide enterprise. An in-demand international speaker on information security, Rushing has presented at many leading security conferences and seminars.

LinkedIn | Blog

Setting priorities in a security practice requires understanding how the business arrived at its current security posture and at the same time, focusing on a vision of where you want to go. "It's a problem we all face," says Richard Rushing, chief information security officer (CISO) at Motorola Mobility. "You have to understand what the business wants, and you have to know what is important to the business."

Depending on the business and the industry it is in, the most important factors might be regulatory requirements, third parties, people within the business, or data assets such as customer data and confidential business data. For many organizations, the most critical pieces include all these things. Rushing says that deciding what is most critical is not something CISOs can do on their own. "This is one of the key things, that going forward, the CISO is going to need help in understanding the business. He will need sponsorship, friends, people he can have honest conversations with about how the business is aligned."

This understanding is fundamental because it goes to the heart of understanding risk to the business, and when it comes to discussing security priorities with executive leadership, risk will be at the center of that conversation. Speaking of the many contending security priorities any large organization faces, Rushing says, "You really have to boil it down to the simplest equations, and one of the simplest is risk."

Rushing points out that although there are many ways to talk about risk, there's nothing simple about quantifying it. "The FUD approach, fear, uncertainty, and doubt, does not work so well. They've heard it all before," he says.

> *When it comes to discussing security priorities with executive leadership, risk will be at the center of that conversation.*

TO QUANTIFY RISK, ASSESS POTENTIAL LOSS EVENTS

One way to quantify risk is by relating it to a maturity scale, with lower maturity equating to higher risk. Rushing explains, "You can show where you rank with the rest of your competitors or customers or industry, where you need to be, and the things you need to do to get there." The same scale becomes a tool for measuring progress by showing where you were before a particular security investment, and where you are now. Although this approach may be more useful in a highly regulated industry like financial services, the fact is, being more mature in framework compliance does not make an organization more secure.

Another approach that has more direct meaning for business decision makers is to compute risk in terms of dollars. This can be a complex calculation involving many aspects of the business that are difficult to quantify, like brand value and real revenue impact. However, a typical enterprise has resources devoted to quantifying risk in this way. Rush advises working with financial professionals in the organization who will be able to help devise dollar measurements for real cyber risk scenarios that must be addressed.

Rushing says that when you are making a request, your presentation must show the ultimate benefit in concrete terms. "You really have to

"An approach that has more direct meaning for business decision makers is to compute risk in terms of dollars."

show how something is going to solve a problem in the real world today," he says. "What advantage is it going to provide, and what is the benefit going to be? It should be something that ties back to a problem or risk, like how many people are getting infected with something, and how many hours of downtime you're going to save by preventing that." Rushing advises being totally prepared with what you want to say, being ready for questions that may come up because of things in the news, and being concise in your presentation. ■

KEY POINTS

1 **Turning risk into dollar figures can be a complex calculation involving many aspects of the business that are difficult to quantify, like real revenue impact and cost of recovery.**

2 **Work with financial professionals in the organization who will be able to help devise dollar measurements for real cyber risk scenarios that must be addressed.**

AN EXECUTIVE LEVEL STEERING COMMITTEE IS CRITICAL TO CISO SUCCESS

KEVIN MCLAUGHLIN

Associate Professor,
American Public University

Dr. Kevin McLaughlin has more than 35 years of corporate and cybersecurity experience. Over the course of his career, he's been involved in creating three cybersecurity operations centers, implementing cybersecurity architecture for three Fortune 500 companies. An army veteran, McLaughlin has led over 800 cyber investigations, was a SWAT team leader, conducted anti-terrorism activities, and has provided solid executive management.

Website | LinkedIn

Before making a case for security expenditures to the C-suite or board, Kevin McLaughlin, associate professor at the American Public University, advises that you first understand what your executives and executive steering committee feel is important. "If you don't have an executive-level steering committee, you need to put one in place," says McLaughlin. The steering committed could include key C-level executives like the CFO, possibly a board member with an understanding of security issues, and key business unit executives. "They are the touch points that allow you to understand the business priorities and make those priorities your priorities."

McLaughlin says the next thing is identifying risk in the organization. "Always keep in mind the old leadership mantra that if it's not measured and tracked, it's probably not getting done," he explains. "When you're pushing risk mitigation, you have to have a way of tracking the mitigation efforts."

Knowing what's important to the business and being able to track your efforts to address it become the cornerstones of your communication strategy with executive-level decision makers. But that's just the beginning. One must also communicate risk while managing communications in a way that enables decision makers to make the right decisions. For instance, how you describe risk has a lot to do with your target audience. "When you describe risk to the board, they're looking at the entire organization," says McLaughlin. "An unpatched network component may carry a high risk from the security team's perspective, but it might not have the same level of risk for the board that has the entire organization view in mind."

> *When you're pushing risk mitigation, you have to have a way of tracking the mitigation efforts.*

McLaughlin also says you need to tie your mitigation efforts to the costs of a crisis, but you can't overplay the fear factor. "You don't want to sound like Chicken Little crying about the sky falling. Your job is to keep the sky from falling," says McLaughlin. "There's already plenty of awareness out there, just from what's in the news all the time. You need to manage the fear, uncertainty, and doubt that your audience already has." Part of communicating risk is talking about its likelihood, but McLaughlin says that can be tricky, because risk probabilities can change from day to day. Also, what does it really mean? "Equifax did not think one unpatched server had a high probability of being hit or was a large risk to their entire infrastructure."

McLaughlin advises using simple visuals that communicate the cost impact of threat and remediation. The higher up in the organization you go, the shorter, sweeter, and more visual it needs to be. But he also says it's important to show the reality behind the numbers, showing how security investments map to real, everyday security threats. "The top execs really do like the Enquirer version of what's happening," he explains. "They want to know what the employees are doing, and how it impacts the business. I tell my team that people really are interested in what we do. That's why they make movies about it." He notes that you don't have to tell it in a way that instills fear. "We had 500 phishing attacks this week. Two of them got compromised credentials and we were talking to the bad guy inside an employee's email." McLaughlin says they like those stories because it makes security tangible. "They understand that it really happens and there's

> "Knowing what's important to the business and being able to track your efforts to address it become the cornerstones of your communication strategy with executive-level decision makers."

a reason we're putting controls in place." Ultimately, though, senior management wants to know if you are protecting the organization. "They're interested in the stories, but it really comes down to, 'Are you protecting us from losing profit, and how are you doing that?'" McLaughlin says,

One other bit of advice—don't go in with a proposal you feel they have to accept. "There's lots of risks, so pick two or three and then have a discussion," he suggests. "Let the board buy into which one should be fixed first. It's always best if somebody from the steering committee goes in and says, 'We have to fix this first,' versus you going in and saying it. Once you get that money, you have to deliver the results that are expected." ■

KEY POINTS

1 **Use simple visuals to communicate the cost impact of threat and remediation. The higher up in the organization you go, the shorter, sweeter, and more visual it needs to be.**

2 **Don't provide decision makers with one solution they must accept or reject. Give them risk and cost choices, and let them buy into what's most important for the business.**

THE CISO NEEDS TO BE A BUSINESS LEADER MORE THAN A TECHNICAL LEADER

SUZIE SMIBERT

Global Director, Enterprise Architecture & CISO, Finning International

Breaking the mold of the typical CISO, Suzie Smibert is making a mark in the global information security community as a leading, innovative, and benchmark-setting C-level information-security executive. She mastered the art of translating complex IT challenges into relevant business discussions, transformed companies' cultures into security champions, and continues to inspire the information security community to embrace a risk approach instead of fear tactics.

in
LinkedIn

Many chief information security officers (CISOs) find themselves managing a security program that is encumbered with too many solutions generating enormous amounts of data. They don't have the resources to use all the tools they have effectively, yet new tools are becoming available that provide more advanced protections. What is a CISO to do?

For Suzie Smibert, CISO at Finning International, the answer is clear. "Simplify," she says, pointing out that the average large enterprise has more than 50 different types of devices used to deliver security services across the organization. "The CISO has to assess his technology overlap, pick one, and rationalize. That's going to help free a lot of dollars. He can self-fund his transformation by rationalizing his footprint." This is important, especially for a security professional who is new to the organization. "The last thing you want to do is to have your first interface with the board or executive leadership going and begging for money," she notes. "That doesn't create credibility or show business acumen."

Eventually the CISO will have to go before the board and make the case for an investment. That's when the CISO needs to be more of a business leader than a technology leader. As a business leader, you need to be able to articulate the business value of what you are proposing, and how it aligns and supports the strategy of the organization. "Once you're asking for money, you're going to need to articulate what's going away as a result of doing this," Smibert says. "If nothing is going away in terms of technology or spend, then it's what is new, the number of people you are going to need to sustain this technology, and the value gained. This is where risk quantification becomes very important, as does being able to show how this technology will reduce risk by a certain factor." »

> *"My board doesn't care how many viruses were thwarted. I need to show effective delivery of that program. How did it help support our strategic objective as an organization?"*

But risk is only one part of the calculation of total impact in a meaningful business metric. Smibert considers total contract value over its life, including the cost of purchase, personnel and resources to support it, and all the gains in terms of technical impact, risk reduction, and other factors like reduced insurance premiums—and even increased business opportunity. Then she calculates its impact in terms of shareholder value. "We reallocate costs by region. I consider if what I'm about to buy is going to have a margin impact on the region. Is it going to cannibalize margin, and therefore reduce shareholder value? If it is, and it's not pretty, I'm not going to ask for the money." On the other hand if she can show that a security expenditure is actually going to have a direct positive impact on shareholder value, then she will make the request. Smibert says that the financial group within the company can help with these kinds of calculations.

If you are to get the money you are asking for, then you have to show that the investment is paying off. "That becomes a risk and maturity conversation for the organization," Smibert says. "My board of executives doesn't care about how many viruses were thwarted. I need to show effective delivery of that program. How did it help further, better, or support our strategic objective as an organization? That's what they really care about." ■

"If you are to get the money you are asking for, then you have to show that the investment is paying off."

KEY POINTS

1. **Eventually the CISO will have to go before the board and make the case for an investment. That's when the CISO needs to be more of a business leader than a technology leader.**
2. **A financial group within the company can help show if a security expenditure is going to have a direct positive impact on shareholder value.**

UNDERSTANDING BUSINESS PRIORITIES IS KEY

GENADY VISHNEVETSKY

Chief Information Security Officer
Stewart Title

Genady Vishnevetsky serves as a CISO for Stewart Title, a leading provider of real-estate services, including global, residential, and commercial title insurance; escrow and settlement services; lender services; underwriting; specialty insurance; and other solutions that facilitate successful real-estate transactions. An established leader with experience in building successful security programs and developing defenses against emerging threats, Vishnevetsky leads security, governance, and compliance programs for global enterprise.

in
LinkedIn

Genady Vishnevetsky, chief information security officer for a global real-estate insurance company, says that any CISO stepping into an overwhelmed security operations needs to take immediate steps to identify gaps and establish priorities. Only then will he or she be in a position to sell a security program to senior management. Vishnevetsky recommends starting with these basic steps:

1. **Adopt a framework that is either prudent or makes sense for the organization.** "Just as a house requires a solid foundation, a good security program needs one. The CISO needs to pick a framework that will be the foundation of his/her program," Vishnevetsky says, pointing out that various industry segments may opt in for a different framework. "It could be ISO 27000, or NIST (National Institute of Standards and Technology), or their shorter version, NIST CSF. If the CISO's in the banking and financial sector, banks are regulated by FFIEC. It has its own framework." Vishnevetsky advises not to rush switching a framework. If the company has an established security program based on an existing framework that meets regulatory requirement and was already approved by management, the new CISO should not change that framework right away.
2. **Perform a risk assessment against that framework.** This involves comparing your existing security posture against the framework you have chosen. Vishnevetsky notes that the outcome of this exercise may be different for every organization. "Their priorities are different, and they depend on other factors," he says. "Things like industry and the sector you're in, regulatory

> *"Regardless of how you spin security expenditures or how you show they enable business activity, risk reduction is how senior management measures the return on their security investment."*

requirements, and believe it or not, even company culture. Based on the result of the assessment, businesses will determine the level of risk they are willing to tolerate, which helps CISOs with their priorities."

3. **Once you identify the gaps with with selected frameworks, start prioritizing.** In doing this, it's important to map your security program to business goals and objectives. "Security should not be a traffic cop, but a business enabler. It needs to help businesses achieve its objectives in a safe and secure manner. You need to understand how the company makes money," says Vishnevetsky. "And you have to know where the crown jewels are that you need to protect. Occasionally you will have to adjust your priorities to meet regulatory requirements. But remember, as your business objectives are changing and threats to your enterprise are evolving, you should make necessary adjustments."

Only after the CISO has established priorities will he or she be able to assess what existing technologies and process are helping to mitigate or reduce the risk. If they are not, the CISO now has the necessary information to present a case the executive team. But what does senior management want to hear?

Vishnevetsky says that upper management is most interested in understanding the risks and what are you doing to address them. Risk reduction is how senior management measures the return on their security investment.

> "My board and audit committee need to know in business terms. They want to know what the risk is to the business."

UNDERSTANDING BUSINESS PRIORITIES IS KEY

Answering those questions can be challenging, because executives want those answers in business terms, not technical jargon. This often requires CISOs to adjust their message to the audience. "My messages are different," Vishnevetsky explains. "It depends on the audience and the level within the company. For example my board and audit committee need to know in business terms. They want to know what the risk is to the business." Vishnevetsky frames his conversations within the context of organizational goals such as company reputation or cost of a breach. "They understand this," he says. "I show progress in these terms, how the program changes user behavior and reduces risk. I keep it at a very high level and tied to the business objectives."

Vishnevetsky says that while it may be difficult to quantify the risk, it is important that executives understand the danger they expose the business too by not applying security and not implementing a structured security system. He also says it's important for CISOs to understand their role within the organization. "As CISO, it's not my job to tell the business what to do. It's my job to inform a business about the risk," he concludes. ■

KEY POINTS

1. **Only after the CISO has established priorities will he or she be able to assess what technologies and processes are in place and if they are doing what needs to be done.**
2. **Don't provide decision makers with one solution they must accept or reject. Give them risk and cost choices, and let them buy into what's most important for the business.**
3. **Regardless of how you spin security expenditures or how you show they enable business activity, risk reduction is how senior management measures the return on their security investment.**

WHEN QUANTIFYING RISK, MAKE IT REAL AND TANGIBLE

SURINDER LALL

Senior Director,
Information Security
Viacom

Surinder Lall is a highly skilled security professional with more than 20 years of experience in the technology field. Lall is one of only a handful of security professionals with an LLM (Master of Laws). This, coupled with his extensive experience and qualifications in the fields of compliance, governance, and information security, allow him to be an effective strategist throughout the security, compliance and governance life cycles.

in
LinkedIn

One management challenge many organizations face relates to the way they have built their security strategy over time. Ideally, you would make decisions based on a multi-tier model of your network that includes perimeter, internal systems, external systems, and mobile devices. You look for the best-in-class technologies and services to secure all those things, and you try to minimize overlapping functions in the solutions you adopt.

That's a great idea, but in the real world of rapidly changing infrastructure, shifting threat vectors, agile business activities, and an evolving perception of risk, it almost never happens quite that way. "Most of the time technologies have been implemented because someone read about them and heard they're good products," says Surinder Lall, senior director of information security at Viacom. "In the security space there is plenty of duplication. You can have three tools doing very different things, but also components of them doing very similar things. That's why you need to be careful."

To rationalize this situation, many CISOs find they must strip away some of what they have, invest in new solutions, and do those things without creating security gaps or introducing new risks and they've got to sell their program to executive leadership.

One way to justify changes is in the context of a maturity model based on standards appropriate for your industry segment. "You need to benchmark the maturity of the existing operation, and build a maturity map of where the organization sits as far as your assessment is concerned. Then you make a business case based on the technologies and the platforms available to fill gaps," Lall explains. »

> *"In the security space, you can have three tools doing very different things, but also components of them doing very similar things. That's why you need to be careful."*

WHEN QUANTIFYING RISK, MAKE IT REAL AND TANGIBLE

Business leadership will also want to see how the program addresses risk, and that will involve measuring risk in a way that enables them to see its potential impact on business performance. This is complicated by the uncertainties around estimating risk cost, and also the fact that organizations in different segments and with different corporate cultures see risk differently. "Not everyone shares the same view on risk," Lall notes. "Some prefer to wait and see what happens. Some will put the money down and say, 'Spend what you need.' It varies from company to company."

To calculate the potential cost of risk, Lall says you have to take many things into consideration. "It comes down to commercial value if an asset is exposed," says Lall. "What will the business lose? You need to factor in the cost of the lost asset, the legal liabilities, PR damage, loss of future business, and in some cases fines." Some industries are more meticulous about estimating risk cost than others, and this affects how you present to senior management. Lall, who has worked in both the financial services and media segments, cites differences between these industries.

The media segment is always seeking ways to monetize assets and has a much higher risk appetite than some other industries. It also has special challenges in measuring risk. Lall says, "The media sector in general has such a diverse set of delivery channels. You're looking at digital delivery, streaming services, billboards. You've got it all going on." This makes it difficult to calculate the value of a loss. One example

> "Not everyone shares the same view on risk. Some prefer to wait and see what happens. Some will put the money down and say, 'Spend what you need.'"

might be the Sony breach from several years ago, in which Sony lost personal data of its employees, digital files of movies, and was blackmailed into never releasing a movie.

On the other hand, more regulated industries like financial services have almost no risk appetite. "The risk posture of that business is as little risk as possible," Lall says. "Everything will be considered critical." He also says they will be meticulous in their questioning about any proposals you present to them. "If you go in with figures, they need to be rock solid." ■

KEY POINTS

1 **In the real world of rapidly changing infrastructure, shifting threat vectors, agile business activities, and evolving perceptions of risk, there are often security solutions with overlapping functions.**

2 **Business leadership wants to see how a program addresses risk. That requires measuring risk in a way that enables them to see its potential impact on business performance.**

YOU NEED TO UNDERSTAND RISK AND MAKE IT TANGIBLE

HEATH TAYLOR

Director, Information Security Compliance
Live Nation Entertainment

Heath Taylor is the director of information security compliance at Live Nation Entertainment. Previously, he was program manager responsible for campus-wide security compliance at UC Irvine and was an enterprise security manager at CO-OP Financial Services. He holds a BS in Information Technology, with a focus on information systems security, from the University of Phoenix, and an MBA from the University of La Verne.

LinkedIn

"The business is always looking to its bottom line," says Heath Taylor, director of information security and compliance at Live Nation Entertainment, and this is just as true when prioritizing security. In the context of security decisions, he explains, "They're looking at the situation and asking if this were compromised, what would it cost in fines? What would it cost in payouts? Versus how much would it be to implement this technology, and the people to support that technology, and the processes to support the people and the technology? What is that dollar amount? From there the business can weigh the factors and make smart decisions."

To answer these questions, Taylor suggests using a risk management framework appropriate to your industry, and that covers the regions where you operate, as a good first step. "By doing that and understanding your regulatory obligations, you can then take a look at the systems and processes you have," he says.

You also need to gain a clear understanding of the business's risk appetite. "You have to know the business and understand what the risk tolerance is within the business," Taylor says. "Understanding all the risk transferral and acceptance is key." With that knowledge, you are then able to look at the business's risk tolerance for each asset, and where those assets reside.

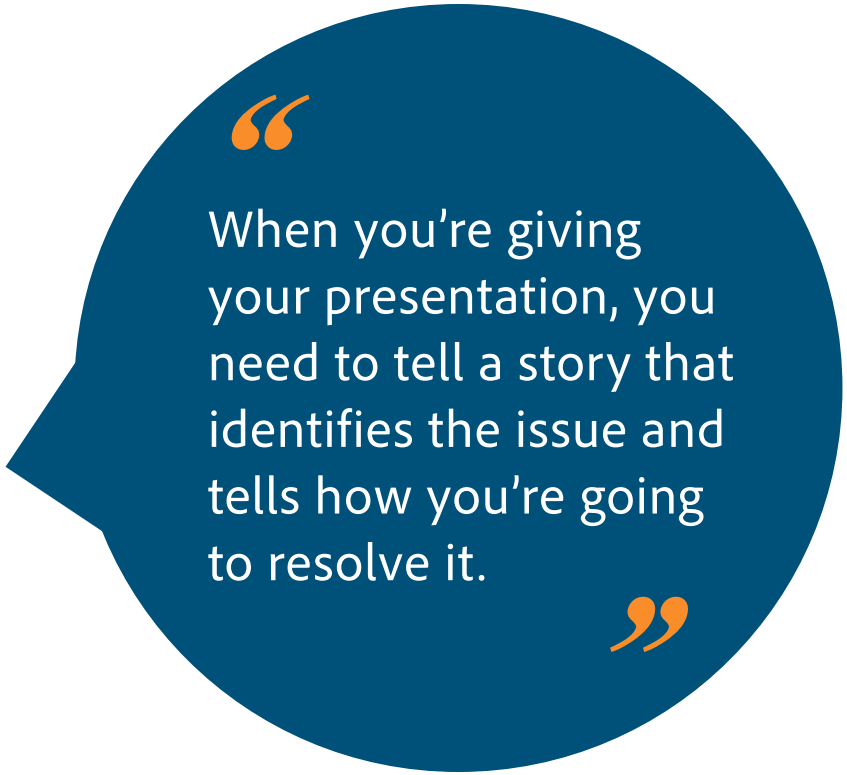
One of the big challenges many CISOs face is quantifying risk in a way that is meaningful to business leaders, who must make risk-based security decisions. "That's always a challenge," Taylor says. "One place to start is to look with the tools that you have. You can look at the CVE [Common Vulnerabilities and Exposures] score. But that can't be the only factor, because focusing on vulnerabilities gives you a very flat view of your risk." He goes on to explain, "You

> *"Ultimately you need to convert risk to dollars for the benefit of the top business leaders, because at the end of the day, they are focused on the bottom line. You have to know the business and understand what the risk tolerance is within the business. Understanding all the risk transferal and acceptance is key."*

need to take that CVE score and put it into your own vulnerability-management system, your own risk-management process. Then, look at each individual item and see what is being done." Taylor says that some organizations take their CVE score, combine it with a predefined organizational risk-management score, add them together, and put them into an easily consumable dashboard or a report.

Ultimately you need to convert risk to dollars for the benefit of the top business leaders, because at the end of the day, they are focused on the bottom line. In addition to considering actual costs associated with data loss, fines, and remediation, this involves many other factors like reputational risk and the probability of a vulnerability being exploited.

In presenting to a board or senior executive leadership, you need to make risks and threats tangible for your audience. "When you're giving your presentation, you need to tell a story that identifies the issue and tells how you're going to resolve it," Taylor notes. Sometimes it's useful to reference past breaches, especially recent ones, to make it fresh for your audience. This is especially effective if you select examples



from companies like your own who are in the same industry segment. Mapping these examples back to your own, known vulnerabilities also helps drive the point home. Then you must bring it back to dollars, such as losing customers, or another business loss.

Taylor advises that in some cases, it's a good idea to bring in a third party as a security partner to dig deeper into assessments of your program or focus on particular issues. "That third party will be able to articulate an unbiased point of view, which can help deliver your message to senior management," he says. ■

KEY POINTS

1 **Only with a clear understanding of a business's risk appetite will you be able to look at its risk tolerance for each asset and quantify the risk.**

2 **In presenting to a board or senior executive leadership, you need to make risks and threats tangible for your audience.**

NEHEMIAH SECURITY

nehemiahsecurity.com

Manage Cyber Risk **in financial terms.**

91%
of boards
cannot interpret their cyber reports

Find out how with RQ: Risk Quantifier

LEARN MORE