FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

SECURITY METRICS & BUSINESS ALIGNMENT

JUNE 2019
KLOGIXSECURITY.COM
617.731.2314

K logix

TABLE OF CONTENTS

SECURITY METRICS & BUSINESS ALIGNMENT

WHAT PATH WILL YOU TAKE TO MAKE THE BIGGEST IMPACT?

To view past issues, visit:
www.klogixsecurity.com/feats-of-strength

Magazine Created By:

K logix

Magazine Contributors:

Kevin West
CEO, K logix

Katie Haug
Director of Marketing, K logix

Kevin Pouche
COO, K logix

Marcela Lima
Marketing Coordinator, K logix

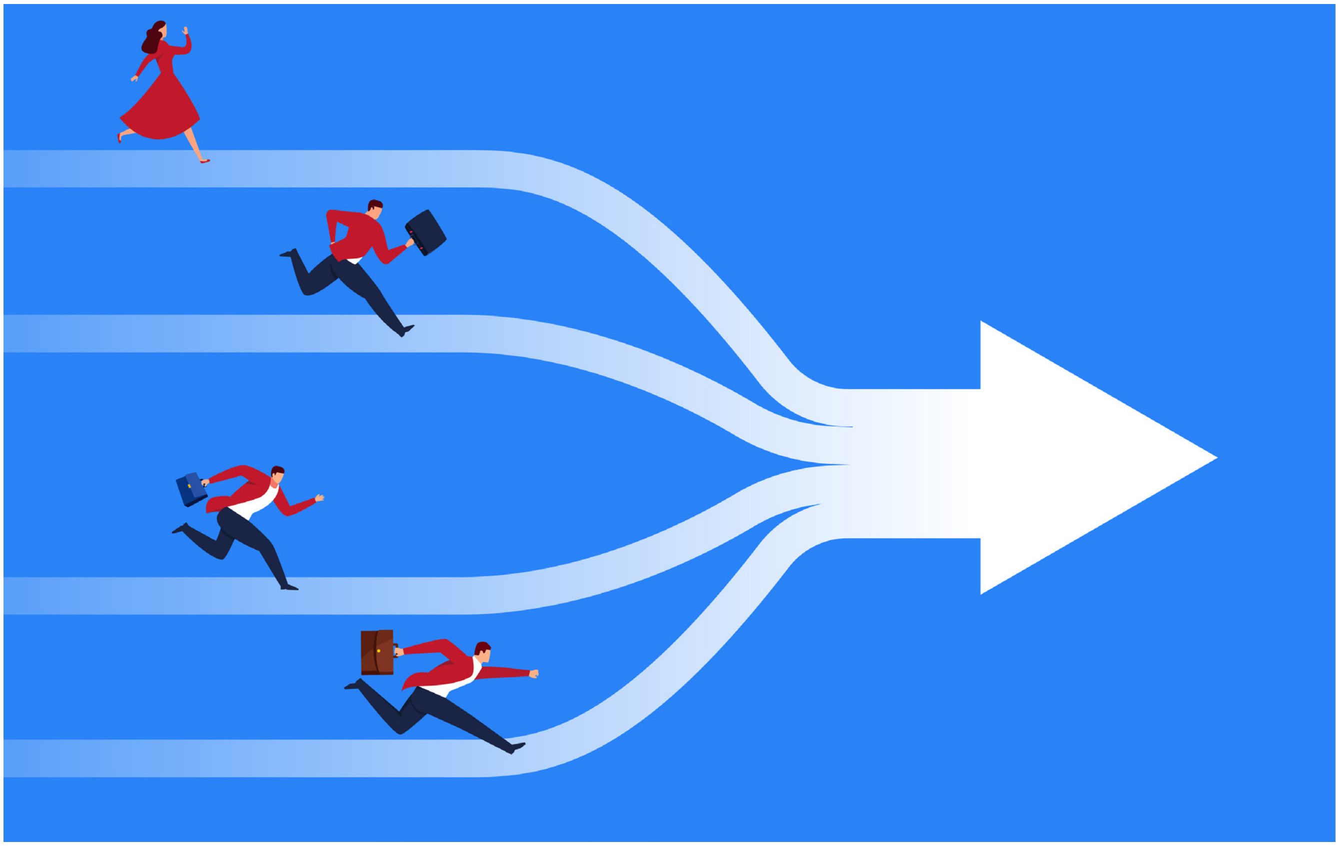
Contact Us:
marketing@klogixsecurity.com
617.731.2314

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication Feats of Strength. Through 100+ CISO interviews, we extract trends in order to provide services that align business to information security.

LETTER FROM

KEVIN WEST

CEO



SECURITY METRICS: ART OR SCIENCE?

Are security metrics an art or a science? To me, they are both. The science of security metrics is a comfortable place for many CISOs and technical-minded people. These types of metrics are fact-based levels of risk and performance-measuring results, yet often technically-driven without context to financial impact, keeping information security siloed from the business. The art of security metrics is utilizing information to gain mindshare with business people and shift thinking towards a unification of security and business process.

In this issue of Feats of Strength, we discuss the power of metrics and how CISOs and the businesses they serve harness this data. The goal is to understand which security metrics best translate to business in order to support the maturity goals being created by CISOs and CIOs.

We chose this topic because for many years, we have asked CISOs and other security leaders what types of metrics they share with their executives to move their information security programs up the value chain and more closely aligned with current and future business directions. When correlating the responses we get, our analyses have resulted in many one-off, unique answers. Some CISOs say that what they track, in terms of specific metrics such as KPIs or KRIs, is based on what they think is impressive or what they're making progress on, not necessarily what boards or other executives want to hear.

The one significant commonality among CISO answers is that there's a disconnect when it comes to what metrics CISOs track versus what metrics their businesses are most interested in. More importantly, security may not be in tune with all business lines and therefore not tracking key metrics that correlate to business transformations.

BUSINESS TRANSFORMATION AND METRICS

By and large today, businesses are transforming and experiencing a technology revolution where traditional processes are challenged, modernized, and better automated with great success. Almost every department within an organization now leans toward the future based on outsourced infrastructure, software, or people to accelerate their time to market. Things are now done significantly faster and easier than before.

With all this transformation taking place, how do CISOs and their information security programs keep pace to secure the future and justify the value they provide? Knowing this may better answer how to frame your security metrics.

K LOGIX: METRICS-DRIVEN BUSINESS

At the core of K logix, we are a metrics-driven business. We believe information security metrics may be leveraged as an avenue to maintain the same pace of transformation, innovation, and growth as the business. Metrics are the common language to bridge business and security. Metrics around alignment of the security program, technology, and people provide a cohesive picture into how well security is keeping pace and where adjustments need to be made.

Security program. CISOs are ensuring security is actively engaged and communicating within all business units to know where their program is against any changes taking place. This level of interaction enables security to extract important business information and fold it back into the security program. CISOs are then able to provide security program metrics around where they are against transformations and provide details about how the security program is changing and where vulnerabilities may be.

Security technology. The same metrics may be formed around technology to understand what technologies are not keeping pace against any business transformations or what can be brought in to accommodate the rate of change. Metrics may be used to understand how to consolidate, automate, and most importantly simplify.

Security people. CISOs are also able to re-tool and re-train their teams as it relates to where their organization currently is and where it is going. Teams are focusing on areas that make the most sense based on the specific transformations occurring within their businesses. Focused team members produce a more impactful security program that is strongly aligned with the business and moving at the same speed of transformation.

METRICS KEEP SECURITY AND BUSINESS ALIGNED

In conclusion, by approaching both the science and art of metrics together, security programs, technology, and people will keep pace with business transformation. This ensures security and the business are close together and moving at the same pace, and result in security gaining credibility, justification, and buy-in.

In this issue, you will read profiles on CISOs who share their approach to metrics. On page 8, John Masserini (CISO, Millicom Communications) shares specific operational and risk metrics he uses to effectively communicate with his business counterparts and board. We are always interested in hearing from our audience about the types of metrics they use and how they impact their program, people, and technology, so please feel free to share with us and help continue this important conversation.

KEVIN WEST is the founder and CEO of K logix, a leading information security company based in Brookline, MA. K logix helps create confident information security programs that align with business objectives.

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

JOHAN HYBINETTE

GLOBAL CISO, VONAGE

HEADQUARTERS: Holmdel, New Jersey

EMPLOYEES: 2,000+

ANNUAL REVENUE: $1 Billion

As a well-seasoned security professional, Johan Hybinette has seen first-hand the evolution of the role of security within organizations, transforming from being a historically siloed department into a more business-aligned and impactful program. He says, “What security has become over the years is an interesting perspective. In most companies, you will find that everything’s siloed, yet security talks to every department or every group. Security is basically becoming a collaboration between all departments and actually enabling groups in communication. Where we are today you find many CISOs reporting directly to the board, or working directly for the board or the CEO of the company. And I think that’s proper because the CISO is a conflict of interest virtually anywhere in the company. But the really interesting thing about security is that today security is kind of the glue between the departments of the company.”

Currently the CISO of Vonage, a leading provider of cloud communication services for consumers and businesses, Hybinette joined the organization because of the opportunity to build and enable the security program. He explains, “The most important thing for me, is to roll up your sleeves and get stuff done. I am typically not the CISO in a very mature organization with everything that works and I just keep it running. I’m a builder and an enabler, that’s my trait. I come in, I build it. There has to be budget there, but really what I’m looking for is executive buy-in and board buy-in. If I don’t have buy-in from the top down, I cannot succeed.”

When Hybinette joins a new organization, he ensure he gets himself out within the business to understand everything going on as it relates to business functions and culture. He strongly believes in having an open mind and working hard to fit in with the corporate culture in order to achieve high levels of success.

JOHAN’S PUNCH LIST

Hybinette believes the CISO of today is more of a risk leader than an owner of controls, and someone required to measure risk continuously. He has a formula he’s named “Johan’s Punch List.” He comments, “It’s really a risk register, we meet weekly on the reporting of risk and see how to progress. You

> *“SECURITY IS BASICALLY BECOMING A COLLABORATION BETWEEN ALL DEPARTMENTS AND ACTUALLY ENABLING GROUPS IN COMMUNICATION.”*

get a score between zero and one hundred percent, it gets reported quarterly to the board and the board sees the highest risks. The report is written in a very high-level way so the board can understand what's going on. A lot of security leaders get too technical. It needs to be high-level. In the beginning when you start in a company, there's a lot of doubt from the board and you must report the risk challenges. You want to become agnostic and gain trust in order to become successful."

Hybinette says it is not just the security team who reports on risk, but every department and every division provides their own reports on risk into the main risk register. These risks are then discussed and evaluated with corporate teams, and they determine if the risk is going up, down, or maintained. Timeframes to mitigate risk are also reviewed, creating a comprehensive view into all risks within the organization.

STRATEGIC GOALS AND CHALLENGES

The top strategic goals Hybinette is working towards are putting security into DevOps and going through a transformation program in 2019. He shares, "Cloud is definitely one of the biggest transformation projects. Companies move into the cloud in some way or another, but my thought is that OT is becoming a really large part of security. Everyone thinks about IT security or information technology, but nobody thought of operations technology and how to make all this work. Cloud is basically the first step, and after the cloud, you go through the containers. After container work, you're getting into serverless. So those are several levels of transformation. It's much more complex than that."

Delving further into what transformation means, Hybinette says, "Another huge part of our transformation is access management. Here's an interesting part of that. Access management cannot be owned by the CISO, it has to be owned by IT. Same with CASB. The CISO will not know who's connected to where, when, and why. Only the stakeholders can do that. And that falls into the IT group that generally controls that. Then the CISO organization now reports on the risks of access management. Also, the CISO organization is architecting access management with IT. So maybe doing more of the risk management, architecting the organization, helping the company architect the proper solution and the compliance, and secure it at the same time."

When asked about challenges, Hybinette says people, more specifically training people, is a large priority for him. He says lack of training is often when breaches occur, especially in instances when someone is not doing their job right or something simple occurs such as missing a line of code. He engages in security awareness training and phishing campaigns where he goes into each group and sits down with the team to educate and share his knowledge with them.

When it comes to security awareness training, Hybinette comments, "Most CISOs are very technical but it's the human factor that you really need to focus on. The security awareness tool is only as good as the people operating it. People are training people. You can actually predict what you're getting, and you know the results are going to be there."

CLEARING THE PRODUCT CLUTTER

On addressing the intense clutter of security product companies in the marketspace, Hybinette says many tout the same message as being leaders while using hot industry buzz words to try to sell their solutions.

He comments, "You need to review them and ask what you want that technology to do for you and how it will work in your organization. After you define that, it's basically a process of elimination. You look them all up, you discount the first round. You may want to talk through the second round, and you go through that and demos, then you take off another big chunk of them and you should only have three vendors that basically evaluate against each other. Is this vendor going to survive? I'm so worried about the startups because they want a big name, such as Vonage, under their belt. They want to be acquired. So, everyone's coming after us or companies like our company because of that. We have a very good legal team to make the property contracts."

ADDRESSING PRIVACY LAWS

As a global organization with international offices, Hybinette says when they addressed GDPR they realized 70% is around legal and privacy, not necessarily technical compliance focused. He continues, "That was the lesson learned and that's part of the GRC investments we did, to track GDPR and privacies. Also setting up a whole new policy set, auditing policies, at the same time to ensure GDPR is being followed. It's very difficult to know when you are GDPR ready. What bothers me a lot is that every company says they're GDPR compliant, nobody's fully GDPR compliant. You can only put the GDPR readiness statement on your website, same for California and the other privacy laws.

WHEN SECURITY METRICS MISS THE POINT

BY GUEST AUTHOR: JOHN MASSERINI, CISO, MILLICOM (TIGO) COMMUNICATIONS

Three-time CISO John Masserini, shares his opinion on the complex topic of information security metrics.

In today's world, many of us have heard of the Body Mass Index (BMI) and likely have had some intense discussions with our healthcare providers about our personal BMIs. The idea behind BMI is that a 'healthy' person of a given height should be within a range of upper and lower weights. A well-intentioned effort to give the general population an understanding about what their 'optimal' weight should be. But looking closely, BMI is nothing more than a metric used by the medical profession to put some type of measurement on a person's weight/height ratio. Unfortunately, the BMI calculation doesn't consider the type of weight a person carries – whether its fat, muscle, or water – only that they have it. Because of the lack of context behind the BMI, it can be misleading around a person's true health status. For example, every world class bodybuilder, all who average 3%-5% body fat, are all morbidly obese according to the BMI. Kind of strange in my opinion.

Now, I'm sharing all of this to prove an important point that every security executive needs to come to terms with: even though they are well intentioned, just like the BMI, security metrics can be horribly misleading.

Don't get me wrong. I am a huge advocate of measuring your security program and leveraging those metrics to communicate risk with all of your stakeholders. That said, all too often those metrics are used for shock and awe rather than communicating important messages around risk.

After countless years of presenting to boards, executives, and colleagues, I've found that I've developed almost a split-personality when I'm asked about what metrics to track. There are metrics that I need to manage risk across my enterprise, and there are different metrics that my executives are interested in. Sometimes they are the same, but most times they are not.

OPERATIONAL VS. RISK METRICS

When running an operation whose sole focus is on defending us against attacks, the kinds of metrics I want collected are of very little interest to my board. I care about ensuring I have enough headroom with my solution as much as the amount of risk I mitigate. We shouldn't be bragging when our solutions are doing what they are supposed to – only highlighting when they don't.

If you feel compelled to talk about the shock and awe numbers, do yourself (and your board) a favor and talk about efficacy – not volume. Telling your board that your anti-SPAM solution is 99.9735% effective means far more to them than saying you blocked a gazillion SPAM emails, and as a side benefit, you get to open up a dialog with them around how no solution is 100% perfect.

Your goal is not to use metrics to scare your executives, but to find metrics that they can relate to. To quote one of the most influential psychiatrists of the 20th century, Milton Erickson once said:

"Every person's map of the world is as unique as their thumb print. There are no two people alike. No two people who understand the same sentence the same way... So in dealing with people, you try not to fit them to your concept of what they should be."
- Milton Erickson

Ponder that for a moment. Most of us deal with boards and management teams which number in dozens of participants. Your metrics need to make sense not to the one person you are speaking to, but the dozen or so board members who all come from diverse backgrounds and experiences. You don't have one different map of the world to deal with, but dozens. Well planned metrics bridge the communications gap that comes with having multiple world maps in your boardrooms.

OPERATIONAL METRICS:

So even after all of this, I admit I do share certain operational metrics with my executives and board.

SOC EFFICACY: Metrics like Mean Time to Close (MTTC)/Mean Time to Resolve (MTTR) reflects the efficiency of the SOC team in resolving events. This is a key indicator of staffing challenges in the SOC and highlights the potential need for hiring or training existing staff. The key is to choose metrics that not only measure risk reduction, but also demonstrate value and effectiveness.

COMPOUND ANNUAL GROWTH RATE OF EVENTS AND INCIDENTS: In the financial world, CAGR is a common term with a well-defined meaning. By using this metric to represent the growth of events, incidents, and attacks, executives understand the reasoning for budgetary investments in the security infrastructure and SOC. Used hand and hand with the MTTC metric.

SOLUTION EFFICACY: The overall effectiveness of the existing solutions. This is where we measure SPAM, NIDS/NIPS, Anti-Virus and any other solution we have deployed. This is also used to show the adoption rate of new measures like multi-factor authentication, privileged access management, and user certification hygiene.

SOLUTION LIFE EXPECTANCY: This metric shows any security solution that has less than 20% headroom is beginning to show a decreased efficiency due to changes in infrastructure, attack vectors, or business functions. Primarily used to set the stage for budgets or capital expenses.

RISK METRICS:

Ultimately, this is the bread and butter of any metrics program. Each of the categories below can leverage the same data collection for both functional risk mitigation strategies, as well as communicating those risks to executives.

ATTACK METRICS: Attack metrics are arguably the easiest to obtain and the hardest to use effectively and the most susceptible to succumb to the pitfall of shock and awe. Here's the thing about attack metrics – while the month-over-month volumetrics are important, most of the rest of it is useless noise. Discuss the new attack(s) we're seeing that we are susceptible to and what we're doing about them.

VULNERABILITY METRICS: The stalwart of the metrics world has to undoubtedly be reporting vulnerabilities. The key to effective vulnerability metric reporting is to relate them to potential financial impact to the company. Do not report a count of generic 5-tier risks (none through Critical) to the board without any insight to the financial impact of your critical systems. Again – avoid the shock and awe, but rather, put these findings into context by associating them with the revenue that could be impacted by attacks impacting those systems.

AVAILABILITY METRICS: All too often, the availability of a system is prioritized well behind the confidentiality or integrity of a system. Have you done a business impact analysis on that 30-year-old system that runs that old Cobol-68 program which just happens to drive 75% of your revenue? Well guess what? The board wants to know you're on it and there's a plan to ensure its upgraded, migrated, or backed up even though there isn't a published exploit anywhere in the world. If you've forgotten what the C.I.A. is, perhaps it's time for a refresher.

REGULATORY METRICS: We all have them – whether its PCI, HIPAA, SOX, or any other government/industry regulatory requirement we have to deal with. When discussing these risks with your board, do not just talk about the gaps you have. Make sure you also articulate the potential fines, especially in this GDPR world, and how those gaps could directly impact the levels of fines faced. It's easy to again fall into the shock-and-awe situation with this, but try to avoid it. Use as much realistic data as possible, especially when dealing with publicly disclosed fines.

So, is your next board meeting going to be filled with fear-inducing, shock and awe, BMI-type metrics, or are you going to focus on communicating those risks that the board wants to hear in a way they want to hear it?

Remember, every person in that room interprets your words in their context – not yours. Make sure your metrics bridge the maps of all the world's before you.

John Masserini is recognized as an industry leader whose expertise across multiple verticals provides a unique approach to delivering an information risk program which drives business focused solutions to today's global information security and compliance challenges. Read more of John's opinions on his blog, Chronicles of a CISO: https://johnmasserini.com

PROFILES IN CONFIDENCE

HIGHLIGHTING PROFESSIONALS LEADING THE WAY FOR CONFIDENT SECURITY PROGRAMS

LUKE MCCONOUGHEY
CISO, Workfusion

HEADQUARTERS: New York, NY

EMPLOYEES: 350+

ANNUAL REVENUE: Undisclosed

> "We have been successful leaving the technical jargon behind and discussing cyber threats as corporate outcomes. With a sound business plan, budget, and staffing, our priorities are attainable."
>
> - LUKE MCCONOUGHEY

Luke McConoughey has worked in every aspect of information security, ranging from satellite cryptography to cybersecurity operations to audit to policy and governance. He says, "I love every aspect of it, it's very interesting to me; there are opportunities everywhere."

Currently the CISO of Workfusion, an Artificial Intelligence powered robotic processes automation platform that automates operations and upgrades customer experiences, McConoughey's role allows him to work at the nexus of cybersecurity, DevOps, automation, and artificial intelligence. This unique position enables him to take on new priorities and challenges. He explains, "We're doing robotic process automation powered by an AI engine. It seems that most AI solutions today are marketing gimmicks, especially in the cybersecurity and IT space. Most of the promising and interesting AI is still on the front office, business development, revenue generation side. But being able to be an early adopter of applying AI to cybersecurity is incredibly exciting."

As the organization's first CISO, McConoughey finds himself equipped with adequate budget, strong support, and innovative opportunities. Before joining the Workfusion team, he carefully evaluated the CISO position, how the management team approaches leadership, the top organizational goals, and how he would fit into the overall corporate mission. While many organizations face challenges around budget, time, and people, McConoughey responds, "We have been successful leaving the technical jargon behind and discussing cyber threats as corporate outcomes. With a sound business plan, budget, and staffing, our priorities are attainable."

Transitioning into a C-level role required McConoughey to take on larger organizational challenges. He comments, "Moving into the C-level, for me, meant focusing on the practical applications of transforming cyber risk into business sense through quantitative risk assessments, automated risk assessments of activities, then setting acceptable risks thresholds and tolerances and where that deviates, and getting additional insights or awareness of what's happening in the environment."

One of McConoughey's current top challenges is getting visibility and understanding of the business operations. He describes this as implementing measurements and starting to quantify aspects of the business itself. This enables him to focus on reducing the threat surface but also gaining valuable insights into activities that are going on and making sure the right controls are in place.

FOCUSING ON METRICS

McConoughey understands the importance of preparing for board presentations by being mindful of key topics board members are interested in discussing. His security program produces operational metrics, he says these are not insightful for board members, and can distract from what truly matters. To have an impactful engagement with board members and executives, McConoughey communicates in dollars, goes into detail discussing probable outcomes, and concisely shares how they've mitigated risk. By doing so, he sets himself and his team up for success and encourages business alignment.

When McConoughey initially started putting together board presentations, he tried to leverage outside sources for inspiration and guidance yet found a lack of readily available information. He says, "I looked to a number of my peers, I searched for 'CISO board presentations' and nobody is willing to share. I was not seeing samples of what works in terms of what is important and what isn't. No one is sharing that learning, that experience, or that scar tissue. That's kind of sad for me. I was able to leverage our internal board presentations for something that had the same ergonomics. I ended up sticking with my intuition and experience."

McConoughey shares different metrics with the board than those he shares internally among his team in terms of varying detail, approach, and granularity. He explains, "The team metrics are much more detailed, things get abstracted into thematic risks focusing on the actual impacts and communicating what's happened versus what was a near miss. It's a lot easier to talk about it in that respect. Here's what happened, here's how much it cost, here's what a mitigation solution would be and why we're going to accept that risk or we're going to fully mitigate that risk. At the executive level it's pretty much dollars. We'll frame the conversation around the type of challenge, how this happens, and what we've done to fix or address it. I also share what we're considering or what we're planning and the residual costs. And if someone disagrees, we talk about what it would take to get further and evaluate the costs."

LEADING A STRONG TEAM

"My current team is five and we're growing and expanding. I worked in China for several months and one of the most important things for me was this concept of "Guanxi", where in China, you have to build a personal relationship before you can get down to business. That was something that helped me be very successful in China and also here building personal relationships and trust, and helping demonstrate that we are successful together and not be a department of "no" or someone that's going to hinder their ability to reach success. Guanxi is my secret," says McConoughey.

When hiring new talent, McConoughey explains, "I look for a balance of soft and technical skills. I don't want someone that's overly technical that is unable to communicate effectively and rationally, I can't have an incredibly smart person talking a foreign language to the leadership. At the same time, during my interview process, I've had HR complaints about how difficult they are, but it's incredibly simple. I want to plumb the depths of your knowledge and get you to say, 'I don't know'. If you make something up, we're not moving forward with you, but if you say, 'I don't know' a hundred times, that's still a big plus in my book as we can teach you, we can help build those skillsets. Overall, I want someone that says they don't know something, who we can train."

McConoughey provides his team the opportunity to attend training courses and conferences, or attain a certification, however he believes certifications don't typically solve many of the problems the industry faces today. He comments, "If there was a certification or a training class, and if only you did this, you would be secure, we wouldn't have the headlines we have today. What I value most is the ability to think through a problem and look at it from many different angles and figure out the best methods to solve it."

> *"In the next few years, AI will have an incredible impact on how we staff, how our tools interoperate, and how we fight badness. I see us sharing entire cybersecurity AI operational models from company to company and across industries, while maintaining confidentiality via differential privacy. This isn't science fiction; this is the science today."*
>
> \- Luke McConoughey

WHAT DO METRICS MEAN TO YOU?

From our in-depth analysis on metrics through countless CISO discussions, CISOs are at a turning point and for those who are not utilizing business *and* technical focused metrics, they recognize the need to start is now. In the *State of Cybersecurity Metrics Annual Report, 2018* 58% of CISOs scored a failing grade when evaluating their efforts to measure their cybersecurity performance against best practices. In that same study, 4 out of 5 companies worldwide are not fully satisfied with their cybersecurity metrics and 43% of respondents indicated some visibility into cyber security metrics but still fail to integrate business stakeholder needs when making critical decisions. When respondents were asked why their metrics fall short, the top two responses were inadequate resources (42%) and time constraints (37%). In another study: *Information Security Risk Metrics, 2017*, 25% of CISOs do not collect and report on metrics, for the 75% that are utilizing metrics, only 40% of their metrics are business-focused.

Here we share quotes we have previously published from CISOs featured in *Feats of Strength*. We asked each of them how they report on metrics and hope their responses may guide some of our readers in the right direction.

"We should really focus on key risk indicators. So how do you prove that you've reduced risk? How many assets do I have under management? How many things are at baseline? And if you can't do that, then don't buy it. So that's how I justify things with management. And I think that actually starts to make sense. As soon as you start talking about risk reduction by dollars, it becomes a lot easier. The biggest complexity was to try to make an argument for visibility because it's not as interesting. It doesn't bring down risk inherently."

– Brandon Swafford, CISO, Webster Bank (original quote from Feats of Strength, March 2019)

"I have 13 metrics that I look at on a monthly basis that either talk about the effectiveness of the program or operations. I'm trying to keep them at a high level and when we talk about metrics, a lot of people like to see colors. So, we talk about being red, yellow and green, but in a different context. Red would mean management needs to take an immediate action, yellow would mean management needs to monitor this area and green means management does not need to take action at all."

- Rich Licato, CISO, ARC (original quote from Feats of Strength, June 2018)

"We report metrics to the board quarterly. We also talk to the board about what our target state is, and where we want to be in the next two years. They absolutely want to know how we stack up against others in the industry and whether or not we're doing the right things."

- Christopher Porter, CISO, Fannie Mae (original quote from Feats of Strength, June 2018)

"I think about two factors. One is collecting true metrics around my program maturity and framework and the ability to define where I am. I need to understand that if I want to move up in maturity what that means from a policy, procedures, and budgetary perspective. The other is technical benchmarking against competitors that I can then use on my own program."

- Richard Rushing, CISO, Motorola (original quote from Feats of Strength, June 2018)

"I think it comes down to ensuring objectives are aligned on what the security organization is supposed to bring to the table. At LinkedIn, the focus is on ensuring member trust with the products we build, securing and hardening our infrastructure, and being resilient when bad things happen. It's really important as a CISO to have a very clear and crisp narrative about what those security objectives are and receive buy in from additional internal stakeholders."

- Cory Scott, Former CISO, LinkedIn (original quote from Feats of Strength, June 2018)

"[CISOs judge progress] primarily by metrics, especially when reporting to senior leadership like the Board. This is where frameworks such as the NIST Cyber Security Framework, help. These frameworks give you a model to communicate to senior leadership what you're doing, why you're doing it, and how you benchmark or measure up."

– Lance Spitzner, Director, SANS Institute (original quote from Feats of Strength, March 2019)

"KRIs are really a great way to do it. Board reporting is a challenge because every board is not created equal. Some companies I've worked for have wanted to tell the board everything. Other companies have been more about making sure that we're giving information that is relevant. Figuring out that balance with your board of how much or how little information is key."

- Patricia Titus, CISO, Markel Corporation (original quote from Feats of Strength, June 2018)

"Like everybody else, we still struggle with trying to find what the best metrics are to convey to the business. At the end of the day, it's about knowing your audience, what's important to them, and what level of detail they like. For example, I do a quarterly governance report where I focus on high-level metrics and initiative updates. I also conduct a Global Information Security report that has far more detailed metrics and operational data."

- David Levine, CISO, RICOH (original quote from Feats of Strength, June 2018)

Q&A WITH NIR GERTNER

CHIEF SECURITY STRATEGIST, CYBERARK

CyberArk is the global leader in privileged access security, a critical layer of IT security to protect data, infrastructure and assets across the enterprise, in the cloud and throughout the DevOps pipeline. CyberArk is trusted by the world's leading organizations, including more than 50% of the Fortune 500, to protect against external attackers and malicious insiders. Today, only CyberArk is delivering a new category of targeted security solutions that help leaders stop reacting to cyber threats and get ahead of them, preventing attack escalation before irreparable business harm is done.

We spoke with Nir Gertner, Chief Security Strategist at CyberArk to learn more about his experience and how CyberArk makes a big impact.

DESCRIBE YOUR 20-YEAR CAREER AT CYBERARK.

This month marks my 20-year anniversary at CyberArk. I was privileged enough to be one of the members of the core team. Throughout the years I've worn many hats, starting as a developer helping build the product from the ground up. Later, I managed part of the development team for several years. I've held the CTO title, then Chief Information Technology Officer, where I had our CISO reporting into me.

About a year and a half ago, I wanted to switch roles to where I am currently as Chief Security Strategist. We thought it would be good to take all of my experience back to the field to have more face time with customers. It's an advisory CISO role where I talk to customer organizations about their security needs, their plans for next year, how to align security and business, and how CyberArk can align with their business. Today my job is customer facing, attending different marketing events and road shows, and of course, internally bringing that back into the company.

WHAT ARE SOME OF THE TRENDS YOU SEE IN THE MANAGEMENT AND PROTECTION OF PRIVILEGED ACCESS?

Privileged account security is number four on the CIS Top 20, and it used to be number twelve a few years ago. There is no place today where privileged account security is not important. Any breach you hear about these days usually starts with a minor incident. In today's market, CISOs think & work under the mentality of assumed breach. Employees will still click on a bad link or open the wrong attachment, because people make mistakes. The difference between having a minor incident and having a major breach is directly correlated to the ability of a hacker to get out of your workstations where they initially landed, and go to your databases, domain controllers, network switches, etc.

Rarely do attackers look for something on your workstation, unless they ended up landing on the CFO's workstation. For me, that is the important place where privileged account security comes in because controlling these administrative accounts is what prevents attackers from advancing. There's so many different paths attackers can take. They can move laterally using weaknesses in Windows, find passwords in a script on your computer, utilize a vulnerable application, and so on. There are so many different types of administrative accounts, and the different ways attackers can move forward are almost endless. Every system has a privileged account. Every device on your network has a privileged account. And so every organization should have a privileged solution.

At the end of the day, we're going to find more of these privileged access pathways that are going to take you from being just a hacker to owning an organization. In the world of IT, there's a shift towards more automated processes. If I'm a hacker, this automated pipeline of development to production becomes a great target for me. They're not going to try to attack the developer's workstation, they attack the pipeline.

It's difficult for a security team or for developers to know the code on one end was changed by the hacker as it was flowing through this automated process before it got to production. There is a whole world today where virtual robots are doing work instead of people. If I am a hacker and I'm able to change what this robot is doing, I am now in control. I don't want to say it will be the next wave because it's already here and it's growing exponentially. As IT moves into that, it's also where we're going to find more security challenges, specifically around privileged accounts.

I'm not against automation, but look how it ties back to security enabling business. It's more dangerous to put in an insecure automated process than to put in an insecure human process. When you have a human involved, we assume that they are the weakest link, but humans can also think. They can see suspicious actions on the screen. But when a robot does their work, nobody is monitoring the screen. So, more automation means less visibility. We wanted automation because it's less people, more money, better revenue, and all of that. But security is so much more important. Humans sometimes make mistakes, but they also find mistakes.

HOW DOES PRIVILEGED ACCESS HELP CISOS WHO WANT TO REDUCE RISK AND ALIGN TO THE BUSINESS?

Different CISOs have different preferences but I would say there are two major areas. One is about risk reduction; how to reduce the maximum amount of risk in a minimal amount of time. And every organization is different. If your domain controllers are going to be hacked, well your company is now owned by them, no question about that. One of the first steps we recommend in our privileged account security program is to take control, monitor, secure, run analytics, with every finger around domain controllers, taking a risk-based approach.

The second is alignment to business goals. If you're an organization that goes through digital transformation and it's all about moving to the cloud, security is not something that holds you back. It needs to be a business enabler. How can you move to the cloud while ensuring you are secure? If your most critical asset is using your AWS console or Azure console, that would be your number one risk. It's making sure we secure that as a business enabler, so you are able to continue to execute on your digital transformation strategy. A privileged security solution helps to secure your most critical assets without holding you back. Security and business really go hand in hand in deciding the right thing for an organization to tackle.

HOW DO YOU DIFFERENTIATE IN A CLUTTERED MARKET?

There's always buzzwords and the silver bullet messaging out there. It's part of the job to understand what's important, what's going to stick. For CyberArk, I'd start with innovation because it's really a core characteristic of any company that wants to survive. If you want to be a successful 20-year-old company, you must reinvent yourself. You must build new things.

Second is the partnership with our customers, and I don't use that word lightly. Many vendors will talk about partnership. I would say that selling software is the easy part of the engagement. Our goal, bottom line, is to have our customers more secure. In order to do that, we have to provide them with tools, set up the software, but then we also have to help them go through the motions of deployment.

One of the things we put in front of our customers is a program that helps them build a successful deployment and then measure it. How do you ensure that you're getting benefits and security? We're talking about risk reduction as a main benefit. How do you ensure that you get that in the first month and don't have to wait for two years of implementation before you can go back to your management and say, hey, we improved security? That's why partnership is extremely important to us.

And then on top of all of that, from a technology perspective, we must be enterprise-ready and our solution has to meet the very tough requirements we get from very large enterprises. It must be a security first approach. It's a security tool, so the tool itself must be secure.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

WE STARTED A PODCAST!

The Cyber Security Business Podcast interviews CISOs and other security leaders to hear their advice about the business of information security.

WANT TO BE INTERVIEWED? LET US KNOW

Learn more about our podcast:
www.klogixsecurity.com/podcast