FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

ASSESSING RISK

WHEN TO ACCEPT, AVOID, MITIGATE OR TRANSFER RISK

IN THIS ISSUE:

DIEGO SOUZA
Global CISO, Cummins, Inc.

FREDERICK WEBSTER
ISO, Blue Cross & Blue Shield of Rhode Island

JOE CORSI
Deputy CISO, Excellus BlueCross BlueShield

JONATHAN SANCHEZ
CISO, TRC Companies, Inc.

SEPTEMBER 2022

KLOGIXSECURITY.COM

617.860.6485

TABLE OF CONTENTS

Assessing Risk *September 2022*

FROM THE *Editor*

Dear Readers,

Assessing risk is always top of mind for security professionals, whether they are aligning with best practices, reporting metrics to executives, or prioritizing resources. Successfully assessing risk means first aligning with business goals, then determining when to accept, avoid, mitigate, or transfer that risk. In turn the overall security posture is strengthened while risk is continually reduced. Organizations approach risk based on varying industry requirements, organizational goals, and the overall nature of their business; there is no cookie cutter approach to understanding security risk. In this issue of the magazine, we spoke with security leaders to better understand how they assess risk.

On page 4, Diego Souza, Global CISO, Cummins, Inc. discusses his overall approach, starting with understanding the environment and business goals, then leveraging a framework to evaluate controls in place. He talks about the benefits of quantifying risk in order to demonstrate business impact.

On page 6, we hear from Jonathan Sanchez, CISO, TRC Companies, Inc., who shares the importance of continuously evolving your approach by revisiting controls, strategy, systems, operations and internal alignment to keep pace with the growing risk landscape.

On page 8, Ryan Spelman, Managing Director, Cyber Risk Consulting at K logix answers trending questions about risk assessments and best practices.

On page 10, Joe Corsi, Deputy CISO, Excellus BlueCross BlueShield talks about the benefits of maintaining an accurate and uptodate risk register that utilizes industry-recognized terms and scoring.

One page 12, Frederick Webster, ISO, Blue Cross & Blue Shield of Rhode Island, discusses how to communicate risk to executives and the benefits of investing in ongoing improvements.

On page 14, we discuss the pros and cons of qualitative and quantitative risk assessments. We share sample heatmaps for each and offer suggestions on which approach might be best suited for your organization.

I hope you enjoy reading!

Kevin West

CEO, K logix

Magazine Contributors

Katie Haug
VP Marketing, K logix

Kevin West
CEO, K logix

Kevin Pouche
COO, K logix

About K logix

Our white-glove approach empowers leaders to advance their security programs and strategically align with the business to reduce risk.

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 hundreds of CISO interviews, we extract trends in order to provide services that align business to information security.

PROFILES IN *Confidence*

DIEGO SOUZA

GLOBAL CISO
CUMMINS, INC.

HEADQUARTERS: Columbus, Indiana

EMPLOYEES: 60,000+

REVENUE: $24 Billion

Diego Souza is currently the Global CISO for Cummins, Inc., an American multinational corporation that designs, manufactures, and distributes engines, filtration, and power generation products and is a leader in the development of clean technologies in the industry like electrified powertrains and hydrogen fuel cell solutions. As a strategic thought leader, Diego focuses on being a business enabler and strong communicator to increase security maturity and continually reduce risk. In taking the role at Cummins, Inc., Diego had an opportunity to strengthen the security program by strictly aligning with business-driven priorities. He says security is part of the organization's DNA and the cyber opportunities in place set the stage for him to help grow the business.

BUSINESS ENABLERS

Diego believes CISOs must understand that cybersecurity should not be a function that sits in the corner of the IT organization. He says security teams and their leaders must be true business enablers who discuss cyber in terms of business risk. He explains, "When we are able to communicate business risk to the board and C-level executives, they are able to see value and why cyber is an important part of the entire organization. Everybody talks about shifting to the left and bringing cybersecurity to the front. I believe cyber should be included from the beginning all the way to the end of the lifecycle. Today we have product needs, compliance needs and regulatory needs and because there are so many different phases of every single program, cyber needs to be included across the lifecycle."

He continues, "It is important to make sure senior leadership from the CEO and C-levels to the Board of Directors, understand why cybersecurity is important to the organization, not only from a response team perspective, but as a business enabler. When organizations are designing, developing, and building products, cyber should be part of those processes."

When presenting to the Board, Diego says many CISOs assume board members don't understand cyber, however it is usually not the case because executives are becoming assume board members don't understand cyber, however it is usually not the case because executives are becoming more security savvy. He says to prepare for questions that tie back to business and operational impact. Often times, board members ask about breaches they read about in the news and if a similar incident could happen at their organization. While these discussions may pose a challenge for some security leaders, Diego believes if you focus on communicating in a way that is understandable and relatable to the board, you will build strong relationships.

"It is important to make sure senior leadership from the CEO and C-levels to the Board of Directors, understand why cybersecurity is important to the organization, not only from a response team perspective, but as a business enabler."

BATTLEFIELD APPROACH

To enhance the visibility of his organization from a cyber standpoint, Diego says they have a battlefield approach which includes the pre, per, post, and when cyber instance.

He explains, “There are four phases of our cyber instances - the pre, the per, the post and the when. Out of the four, three of them we can control, but we cannot control the when. We can control the pre, per, and post. The pre is underlining infrastructure visibility, making sure we have all the necessary processes in place to be more predictive about cyber events so we can take proactive actions versus reactive ones. We are focused on moving to a predictive, proactive organization, leveraging AI capabilities, leveraging behavior solutions that can help us to predict potential incidents. The per is our ability to respond as quick as possible. The post is really making sure that we learn from events and how we fix the whole process so it doesn’t happen again.”

Diego says he never promises that an organization he works at will never get compromised, but he does tell leadership that if it does happen, they will be ready to respond as quickly as possible to minimize business impact.

ASSESSING RISK

To truly assess risk, Diego says you must start with understanding your environment and the business goals in place. First is classifying risk through a framework like NIST to evaluate the controls in place. Then is prioritizing those risks. Diego comments, “We do self-assessments to assess risk that provide us a cybersecurity score to see where we are from the traditional one to five. Self-assessments are typically conducted to monitor where we are from a maturity and risk perspective. We also bring external parties in to provide a different evaluation of our security program. They tell us where they are seeing gaps, and which areas to focus on.”

Diego says it is important to focus on the bigger risks first, especially those that impact the company from a financial or operational perspective. These might even include risks that could potentially impact the overall brand and its reputation.

Quantifying risk is vital for Diego to run a successful security program because it enables you to demonstrate direct business impact. For example, if a system goes down for a certain number of hours, the impact to the manufacturing line will be a specific dollar amount in lost revenue. He explains, “Quantifying risk helps us measure risk from the business side and drive that message back to the C-levels of the company. However, sometimes you cannot quantify risk, so you must qualify it. For instance, a potential branding impact. If a cyber incident happens at your organization and it becomes part of a news cycle, it might impact your stock price. You can’t quantify how much the stock will drop but you need to understand the impact to your business if that happens.”

“I really focus on people. I make sure I invest in them and have open communication in my organization. There is no hierarchy from a relationship standpoint, I have an open door approach with my entire team, so they can get time with me to discuss anything.”

GROWTH

Diego classifies himself as a people-centric leader. He explains, “I really focus on people. I make sure I invest in them and have open communication in my organization. There is no hierarchy from a relationship standpoint, I have an open door approach with my entire team, so they can get time with me to discuss anything. They have reporting lines, however, they have the freedom to talk with me at any time, and I feel that building up those relationships creates a much healthier environment and people want to stay. Especially in today’s market that’s so hot for cybersecurity professionals. I joined this organization because I knew my team would be equipped with the necessary tools, knowledge and processes to execute their day-to-day work.”

To continue to grow as a leader, Diego says he focuses on being a good listener. He listens to what his team tells him and what his stakeholders tell him so he can learn and improve. He is also very engaged in the security community. Conferences are a great way for Diego to meet with peers and share information with one another, whether it is current challenges they are facing or tools they are investing in, it all helps improve the overall maturity of security.

PROFILES IN *Confidence*

JONATHAN SANCHEZ

CISO
TRC COMPANIES

HEADQUARTERS: Windsor, CT

EMPLOYEES: 6,000+

REVENUE: $1.5 Billion

Jonathan Sanchez is currently the CISO for TRC Companies, Inc., a global firm providing environmentally focused and digitally powered solutions across key markets which address local needs. Now over three years into his tenure, he has established strong communication between security and the business, built his team, and continued to reduce risk through a business-focused, strategic approach.

Jonathan's first role in security began as an intern at JP Morgan, where he worked on intrusion detection systems and data loss management projects. He quickly realized he had a knack for problem solving and was promoted to the global incident response team. He comments, "That's where the rubber really met the road. I already had the foundation built for cybersecurity within my previous role and moving up to incident response forces you to do everything from soup to nuts. Being a global team, we were on call 24/7, we built everything you could think and worked with teams globally to ensure that we were performing cyber correctly and continuing to pioneer the lead."

During his time at JP Morgan, he acquired an undergraduate and master's degree in Information Technology/Information Management from Syracuse University with certificates of advance study in Information Security and Telecommunication. After spending five years at JP Morgan, Jonathan moved to BNY Mellon to help them develop their cyber department, growing the team from eight to over 150 people, and increasing security maturity. After three years, he decided to leave the highly regulating banking world and move to TRC Companies, Inc.

COMMUNICATING IN BUSINESS TERMS

Jonathan believes successful CISOs align themselves to the business and are able to clearly articulate the financial impact of security. He says, "Being able to speak in terms that executives and the board understand is important. Leaders receive information in different ways but the key to successfully communicating is by understanding your audience. Boards deal in business terms, management terms and financial terms. You have to be able to communicate that cyber incidents can lead to the firm potentially losing millions of dollars. This is what gets their attention. Cybersecurity doesn't make money as it's not a revenue generating function; however it saves money and money saved is value earned. The board understands what risk is and its potential impact, but until you help them understand what it means to the bottom line or from a cost perspective, they don't easily associate or simulate what it is from a one-to-one perspective. Cybersecurity can be a costly function but being able to right size investments and provide ROI's by deploying cyber solutions, business functionality and uptime are enhanced."

Jonathan says it is vital to show KPIs and metrics that demonstrate how cyber is aiding the business and the maturity of the overall program, and resiliency in responding to potential threat actors. Having these types of metrics demonstrates improvements over time and highlights areas of weakness and strength. Presenting to the boards and executive audiences will require a mixture strategy document, revealing overall strategy, potential key threat areas to mitigate risks and threats identified. Additionally, including visuals for the executive dashboard, which leverages RAG (Red, Amber & Green) rating indicators helps provide awareness from a criticality perspective.

RESPONSIBILITIES

Anything cyber-related falls under Jonathan's umbrella of responsibilities. Part of his role is overseeing their internal controls, how they manage employees and the data they have access to, as well as external risk management and third-party governance and compliance. Jonathan believes data is the lifeblood of the organization and spends time working with the business to determine if the right controls are in place around how data is being used. He says, "I spend a lot of time working with the business and understanding what they're doing with some of the data to ensure that we have the correct cybersecurity provisions to manage data from a threat perspective. We make sure we understand where the data is living - at rest or in movement, and how to securely transfer to make it available to clients or project party

members that are outside of our organization."

Vulnerability management also sits under Jonathan, an area his team focuses on, especially as it relates to reducing the risk landscape. His team also manages incident response and digital forensics by holistically managing any incidents. Another area of responsibility is mergers and acquisitions. He explains, "Whenever we're evaluating the possibility of looking to expand by acquisition, I'm responsible for evaluating their cyber posture, the company data and understanding the potential risk to our organization. There's a lot of due diligence required to ensure it is done correctly before providing any type of signoff and commit to moving forward."

Jonathan and his team are also involved in digital innovations, especially as it relates to building applications. Security must assess risk around application development and ensure mitigating controls are in place to maintain strong security posture with layered defenses.

In terms of the most current focus area, investing in cybersecurity awareness and training is paramount for Jonathan to maintain a strong cyber posture. He comments, "People are your top asset, but they're also your biggest risk. Understanding cyber risks are important but understanding user experience and their interactions with the environment are where the biggest risks are faced. Arming your users with the appropriate tools, knowledge and technology is only half the battle since vulnerabilities are exploited typically due to human error or oversight."

He continues, "Being able to manage the synergies between people, process and technology when addressing cyber threats are all equally important. No system is perfect, but you must have policies, process, and standards in place, which help guide users but also educate and train employees on best practices, while the right technologies are deployed to provide a safe and secure environment. We spend a lot of time training our employees to keep them safe from things like phishing attempts. Being able to train your users and make them aware of what they're up against or what they should be seeing makes it a lot easier for them to make the right decision. We put metrics in place from a baseline perspective, or phishing click rate, so we continue to improve our efforts to drive down the potential risk exposure."

ASSESSING RISK

Jonathan says risks vary across a widespread spectrum, so it is critical for security leaders to understand the different types of attacks and the controls in place to help mitigate or protect the organization. He explains, "Security isn't a one-stop shop, it requires continuous evolution and diligence, so it is important to revisit your controls, cyber strategy, systems, operations and internal alignment goals to keep pace with the growing risk landscape. Attacks are becoming more sophisticated, therefore being able to think like an adversary helps with your ability to strategize and protect your company's assets. CISO's not only need to focus on risks which are currently applicable but being able to be proactively prepare not only for local threats but situationally being aware of risks which can impact business due to current events."

He continues, "Organizations could face 90 to 1,000 risks, but are each and every one of those really pertinent to your organization? If you take a step back and you wrap up all the possible issues and systems together with your strategy, it will help you articulate what your current risk climate looks like, or what you're being faced with compared with the actual internal resources you have in your possession to help fight the good fight."

To do this effectively, Jonathan believes it is imperative to understand qualitative risk analysis. This approach helps to understand the critically of an impact from a financial and risk perspective. It focuses on measuring the likelihood and the impact to determine severity, then recording the results in a matrix. The matrix helps communicate the overall risk profile to the board and business executives. The overall risk profile to the organization provides cybersecurity maturity and preparedness.

Jonathan explains, "We try to do a yearly assessment for TRC and a full sweep with our penetration testing as well, to ensure that we're managing our network and understand what we're up against. We have moved to a quarterly evaluation from a control perspective to understand where we are seeing vulnerabilities. It helps us understand what we can do better to ward off bad actors and eliminate traffic from high-risk areas. We also have bi-annual audits internally to make sure that we're managing permissions and access controls efficiently. For example, we need to be able to track and monitor if a user internally transfers, therefore we'll need to re-provision their access, because risk happens at all levels, it just depends on how much risk you're willing to absorb and how you plan to manage it. Users are your top asset but biggest threat and at times don't even realize they have made a mistake."

GROWING AND DEVELOPING AS A LEADER

Jonathan says, "Cybersecurity requires commitment and passion to growing within an ever-evolving industry. The fascinating part about working in cybersecurity besides the potential to either keep you up late or get you up early is that there will never be a dull moment. In order to be successful, it requires dedication to your craft, willingness to learn and the ability to be flexible. Managing cyber events requires strong use of communication, coupled with soft skills and the ability to work as a team under duress. Outside of the everyday work activities, which can require you to become an SME (Subject Matter Expert), I think its critical for all cyber employees to stay relevant, attend conferences and successfully acquire relevant certifications."

To grow as a leader, Jonathan attends conferences and believes in the value of learning about niche topics, new cutting-edge technologies and coming trends. He says, "I'm currently in the process of working towards two new industry leading certifications. I personally enjoy attending conferences focused on specific topics with fellow CISO's and attending roundtables to discuss trends seen in the wild."

Q&A

WITH RYAN SPELMAN
MANAGING DIRECTOR of CYBER RISK CONSULTING, K LOGIX

RISK ASSESSMENT QUESTIONS ANSWERED

The scale of what risk assessments cover varies based on the provider, in your opinion, what should impactful risk assessments include?

While risk assessments vary by scope and methodology, some focus areas are common across all types. All risk assessments must address the risk "equation"; roughly, threats times vulnerabilities times impact equals risk. A risk assessment must consider the threats to an organization, which may be sector or enterprise-specific. Are they more at risk from nation-state interest? Are criminal syndicates hitting the industry hard? Are there certain personalities involved in the organization that draws the interest of hacktivists? How are their controls structured? Are their policies in place? Do they embrace cyber hygiene? What happens if the controls fail? What happens if the controls that are protecting sensitive data fail? It must explore where the organization is lacking in cybersecurity defenses and consider the cost to the organization if threats were to act on those vulnerabilities.

What are the steps of a successful security risk assessment model?

A successful risk assessment model solves that equation in a manner clear to the organization and provides prioritization to address the level of risk. Often it will be based on a specific cybersecurity framework such as NIST or ISO, or aligned with a specific cybersecurity regulation such as NYS-DFS. Ultimately, it must be a clear and coherent model for the organization to understand the process and the output.

What challenges do risk assessments help solve?

Most organizations have a general sense of their cybersecurity posture. They know about bad decisions they have had to live with, shortcomings of their systems, and challenges that others in their sector face. Risk assessments allow the organization to consider its posture through the lens of risk, which can be clarifying and objectifying. An organization may conceptually recognize that poor software development management is a risk for them. However, if a risk assessment identifies that as an area of concentrated risk such as the types of data they manage on that software, it can make this risk more tangible. Organizations know where they have problems: the priority of the problems is often the unknown factor.

Why are regular security risk assessments important?

Risk changes. Threats shift, new vulnerabilities are introduced, and important systems change in their impact prioritization. Organizations that regularly perform risk assessments (at least every two years) can adjust their plans to address changing variables.

What is the value in a third-party conducted risk assessment vs. an internal risk assessment?

I compare it to the challenges of self-editing. When you review your work, you are prone to fill in gaps, make assumptions, and fail to see what it looks like from the outside. An external reviewer will make fewer oversight mistakes and provide the added value of non-bias. They are not attached to specific projects or have a stake in

outcomes internal teams might have. Additionally, an external reviewer can leverage experience assessing similar sizes or types of organizations and help an organization better understand threats and possible impacts.

How are security leaders using risk assessments to justify budget requests?

Risk assessments let security leaders organize their investments by risk, which is a very compelling way to indicate prioritization. Risk isn't the only justification; sometimes you need to make investments to support business needs or meet an obligation. However, when a security leader is asked, "Why are you spending money here," a risk assessment identifies the need and how the investment will address the need, putting them in a much stronger position.

Where do risk assessments and regulatory maturity compliance overlap?

Risk assessments and regulatory maturity compliance assessments overlap because both are looking to assess the strength of controls. In maturity compliance assessments, the focus is on the controls concerning the expected level of regulatory or framework maturity. This is important, especially when addressing regulatory or stakeholder concerns. Where a risk assessment differs is that it will analyze the maturity of the controls in light of the additional variables such as threat and impact. This analysis adds the appropriate prioritization, which is critical for planning remediation efforts after an assessment.

How should security leaders leverage risk assessment results in executive and board-level meetings?

The first thing everyone should consider with a risk assessment is what the output will tell executives and board members. Is the risk high because the threat environment is high, my controls or weak, or the impact is significant? It is key to reverse engineer the top level (number of high-risk findings, etc.) and explain it in light of the organization's risk story. The best security leaders can use a risk assessment to justify further investments, support current programs, and reduce liability if larger business decisions incur risk. Risk is part of all business decisions, and risk assessments allow security leaders to talk about cyber security risks with greater clarity, evidence, and rationality.

How does K logix help?

We offer white glove security risk assessments custom tailored to customer-specific requirements. Our assessments are mapped against industry standard frameworks and informed by years of in-depth experience. Our goal is to help organizations best identify, act and improve on what they are doing in their security program. We can leverage an array of lenses that apply to whatever security challenges they are currently facing, whether is it the cloud environment or regulatory compliance mapping.

Ryan Spelman has over 15 years of experience in homeland security and cybersecurity. He is currently K logix's Managing Director of Cyber Risk Consulting, focused on helping organizations navigate complex cyber risks. Ryan previously held leadership positions at Kroll, Center for Internet Security (CIS), and New York State Senate Committee on Veterans', Homeland Security and Military Affairs. He can be reached at: rspelman@klogixsecurity.com.

PROFILES IN *Confidence*

JOE CORSI

DEPUTY CISO
EXCELLUS BLUECROSS BLUESHIELD

HEADQUARTERS: Rochester, NY

EMPLOYEES: 3,500+

REVENUE: $6.6 Billion

Joe Corsi majored in Computer Science during college because he felt it was a forward leaning industry and something that would set him up for success in his career. After graduating, he worked in the US Army for seven years as an Officer. For the first four years he served as an airborne paratrooper before ultimately moving into the role of a Cyber Intelligence Officer assigned to US Army Cyber Command. He explains, "Getting into cybersecurity was exciting because the Army was just getting their feet wet from a security standpoint, so everyone was essentially learning together. We had very little internal training available at that time and therefore utilized content provided by third parties such as CompTIA, ISACA, and ISC2."

Early in his military career the Army provided many courses focused primarily on leadership. When Joe graduated US Army Ranger school he went through intense leadership training that helped refine his skills and prepare him for the next step of his career as a leader within the cybersecurity industry.

After leaving the Army, Joe began working within the cybersecurity team at Paychex Inc. where he quickly moved into leadership roles while gaining valuable tactical and strategic experience. After an opportunity at Excellus BlueCross BlueShield opened, Joe excitedly took on the Deputy CISO role, with a focus on identity management and security architecture while also supporting the overall security program.

THE ROLE OF A DEPUTY CISO

Joe says CISOs have become increasingly responsible for managing upwards by reporting to the C-suite and the board. He comments, "The role of a Deputy CISO is to assist in keeping the overall organization running efficiently whether that be assisting in the handling of major incidents or leading large staff events. A Deputy CISO is like having a Chief of Staff role within your organization. It's a valuable position and one that I believe helps keep the department moving forward when the CISO must focus on so many additional responsibilities related to the business."

According to Joe, Deputy CISOs gain vast experience working across all domains of cybersecurity and their core value is in assisting each area to allow the CISO to focus on larger strategic initiatives and executive reporting. His day-to-day work varies greatly, exposing him to all areas of security and business, from leading his own team initiatives to assisting in the preparation of board materials on behalf of the security organization.

MEASURING AND ASSESSING RISK

Joe believes measuring risk starts with using a well-documented framework and leveraging it to re-assess on a reoccurring basis. He says, "Governance, risk, and compliance is a significant portion of our organization responsible for maintenance of our policies and standards and takes the lead in managing our relationship with our external Audit, Legal, and Risk partners. One additional key component of this group is maintaining an accurate and up to date risk register utilizing industry-recognized terms and scoring. I don't think enough organizations utilize well-documented concepts such as Annualized Loss Expectancy (ALE) and Annual Rate of Occurrence (ARO) when determining the best ways to manage identified risks to the company. These concepts are helpful when trying to determine if the work to reduce an identified risk outweighs the costs that may occur if the risk is actually realized. Organizations also have a tendency to forget that you can also accept, transfer, and avoid risk which should all be options considered as part of the larger risk management process."

Joe says the primary value of continuously measuring risk

is that it helps cybersecurity teams remain focused on areas of most importance to the organization. With new projects and priorities popping up on a regular basis, it is important to ensure your finite resources are focused on areas of higher risk where reduction can occur in an effective manner.

SPEAKING IN BUSINESS TERMS

To effectively present and communicate with executives, Joe says there must be a balance of explaining clear and concise metrics while also utilizing some amount of active presentation skills. He explains, "Knowing how to convey what can sometimes be a complicated and nuanced technical thought to non-technical audiences can be incredibly difficult. I've seen senior leaders struggle when talking to other leaders outside IT about certain topics because they struggle to avoid technical terms or jargon. Ultimately you must be able to tie your points back to something your audience is familiar with such as business goals and objectives."

"I've seen senior leaders struggle when talking to other leaders outside IT about certain topics because they struggle to avoid technical terms or jargon. Ultimately you must be able to tie your points back to something your audience is familiar with such as business goals and objectives."

He continues, "Just as important as conveying a clear message is being concise and purposeful with your message. Your ideas can get lost, and you can find yourself being uninvited to meetings if you are seen as somebody who goes off-topic or conveys a long thought with no specific ideas for action. The goal is to have a seat at the table and maintain that seat. Even better if you can find yourself continuously requested to come back because they know it will be an important and well thought out message and a good use of their time. You are successful if you've appropriately communicated risk and achieved any desired outcomes relative to the audience whether that be for awareness or action."

CONTINUING TO GROW AND LEARN

Joe approaches leadership with a flexible mindset and core ability to adjust to the specific needs of those that he leads. When hiring, he focuses on finding individuals with a core set of values and a balance of soft and technical skills. He says, "If you give me somebody that is humble, hungry, and smart, I will find a place for them in my organization. That's not to say that technical skills aren't required in some areas. There are certainly positions within every security team that call for those talents. However, often I find myself looking for people that can communicate clearly and are self-starters that can get work done without having to be supervised. Once I've got a team of those people, the focus shifts towards making them comfortable within their core area of responsibility whether that be through mentorship, peer-review, or training. In my experience if you have individuals with a strong core set of soft skills, most are able to pick things up relatively quickly only a few months into the position regardless of previous experience."

For Joe, peer groups are an essential part of his growth and learning as a security leader. He comments, "Creating networks for information sharing can be seen as a force multiplier. No single organization has all the answers, best practices, tools, etc. If I'm struggling with a particular problem within my own group I know I have the option to reach out to ask others for help. Being able to quickly contact a trusted group of peers on a particular topic is extremely valuable. I can ask them which vendors and tools they prefer or if they've improved a particular process recently. Ultimately this helps me feel like I'm not in this on my own and ensures that I have support whenever needed. Giving back to the community is also important and I try to do that as often as I can."

PROFILES IN *Confidence*

FREDERICK WEBSTER

INFORMATION SECURITY OFFICER
BLUE CROSS & BLUE SHIELD OF RHODE ISLAND

HEADQUARTERS: Providence, RI

EMPLOYEES: 760

REVENUE: $1.7 Billion

Fred Webster says the first few years of his career began at the ground level, working on help desk support tickets, fixing desktops, and troubleshooting laptops. He then moved into server administration, application support, database administration, and other highly technical areas. It was in this work that he gained exposure to project management, a field he felt compelled to explore because he was able to apply a consistent methodology across a variety of problems. His work as a project manager at a managed service provider provided a gateway into information security. He began learning the basic principles of information security before taking on his first official security role as Vulnerability Management Program Manager at CVS. He ran the vulnerability management program and applied project management principles to information security domains. His job expanded to include configuration assessments and positioned him in a managerial role taking over large components of the security operations department.

After leaving CVS, Fred worked at NTT delivering their managed security services to clients in North America. As a senior leader, Fred was a key management contributor responsible for the successful delivery of all managed security services. After spending over four years in this role, Fred moved over to Blue Cross & Blue Shield of Rhode Island (BCBSRI) as Director of Information Assurance, Business Continuity where he was exposed to the policy, risk and governance oversight, something he feels was missing in his previous experience. He was then promoted to the Information Security Officer (ISO), reporting into the Chief Risk Officer.

INFORMATION ASSURANCE AND SECURITY OPERATIONS

As ISO, Fred has two main programs he oversees – information assurance and security operations. From an information assurance perspective, Fred leads third-party risk management, security awareness and training, information security risk and governance, cyber threat and security incidents, and policies and standards.

Managing third party risk management includes assessing vendors and monitoring vendor risk. Fred explains, “We want to make sure our third parties are following best practices and they meet our contractual requirements. We are able to calculate a risk score for all vendors that receive sensitive data. We also use a third-party vendor that monitors the infrastructure and footprints of our vendors for potential risks and security threats.”

BCBSRI’s security awareness program comprises training on an on-going basis, whether it is onboarding a new employee or ensuring associates with privileged access understand their responsibility to keep corporate data secure. Fred says they engage with employees throughout the year, with a heavy focus during cybersecurity awareness month. They collaborate with the compliance team during compliance week, and regularly with the human resources department to ensure they work on various projects with shared goals.

> “I want to enable each team member’s strengths while helping them develop their weaknesses. My approach, and I think this mirrors the overall BCBSRI approach, is we trust that our associates are making the right choices and doing right by the organization.”

To ensure the security program engages in shifting left, Fred and his team have oversight into the RFP or RFI processes as they relate to information security. He explains, "In an attempt to shift left, we want to be at ground level so we can inject security requirements but also help the business assess vendors that are being selected. We want to make sure the business makes informed decisions, and we help them do that by identifying risk within vendors."

Fred and his team manage security risk and governance in accordance with all policies and standards, providing advice to leadership on risk levels and acceptable thresholds. Also, the cyber threat and security incident process provides external threat intelligence, countermeasures within their environment and management of the third-party SOC that receives all logs and triages alerts. This team investigates any security incidents reported internally. Lastly, policies and standards related to information security are regularly updated and drafted by Fred and his team, where they work closely with the business to ensure goals are met and security is maintained.

Security operations includes managing all security tools and platforms from multi-factor authentication, vulnerability scanning tools, antivirus, or anything that has a security agent. They are responsible for making sure those agents are doing their intended jobs and running smoothly.

FOCUS ON THIRD PARTY RISK, IDENTITY, AND RETENTION

Some areas of focus for Fred and his team include third-party risk, an area most security programs are currently concentrating on due to heightened and ongoing risk posed by vendors outside of an organization. Fred says, "We have lots of confidence in the core components of the program but every time there is a third-party breach or security incident, I look back and we might have given them a good score so we try to understand what other components we can add. This will help show us indicators of increasing risk or potential risks that we might not be seeing today."

Identity and access management is an area Fred and his team plan to continue to focus on. He explains, "You're not talking about servers and firewalls anymore, you're talking about someone's identity and the privileges that that identity has. So identity and access management is an area where there's an opportunity for us to provide more governance and more oversight."

The ability to retain and grow their team is another top priority for Fred. He comments, "We did well retaining people over the last two years. It comes down to our culture and the environment we have cultivated. But there is always more work to do, and I want to make sure our staff is fulfilled, and they are doing the work they want to do."

ASSESSING RISK

Fred explains, "We communicate risk to executives through our enterprise risk management program. Cyber has been the top risk of organization for last three years. As part of that risk program, we assess the various components of cyber risk on an annual basis. Our goal is to always improve, and we continue to tweak that process. For example, we might go back through our scoring techniques to really highlight the underlying risks and map them back to what risk means to the organization."

LEADING WITH TRUST & EVANGELIZING SECURITY

Fred says his approach to leading a team is based on being a good coach and providing support as needed. He says, "I want to enable each team member's strengths while helping them develop their weaknesses. My approach, and I think this mirrors the overall BCBSRI approach, is we trust that our associates are making the right choices and doing right by the organization. That's a key component to my leadership style. My primary job is to support them while I keep an eye on the business results in driving the business outcomes that we want. I am fortunate to have a strong team so it's really just guiding the ship that is already heading in the right direction."

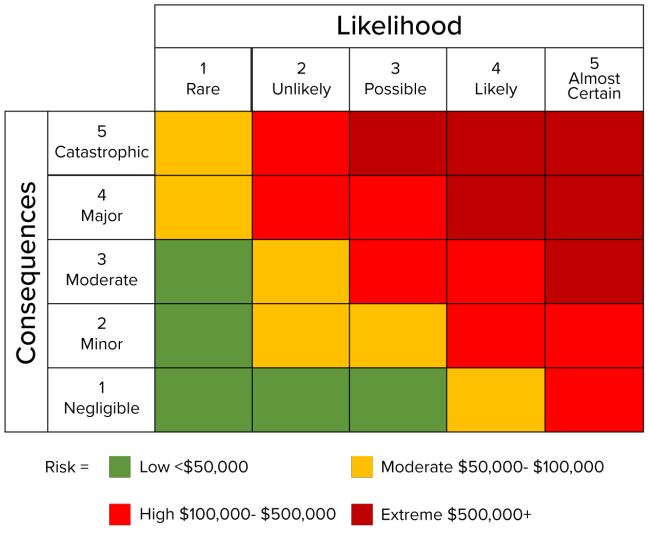
Fred adjusts his approach when he is speaking with executives outside of his department. He says he focuses on being an evangelizer for information security, discussing it across the business and making sure everyone understands the value. He shares, "It's important to not only communicate in terms the business understands, but in terms they care about. Some groups might not care as much about cost, but they care a lot about reputational impact, so understanding the audience and mapping back to the business conversation is important."

Quantitative vs. Qualititative Risk Assessments

By Katie Haug, VP Marketing, K logix

After speaking with CISOs and security leaders on how they assess risk, it's clear there is no one size fits all approach. Evaluating risk varies based on organizational goals, corporate missions, and industry-specific requirements. Depending on maturity, security programs may take either a qualitative or quantitative approach to assessing risk. Some organizations prefer to evaluate solely based on qualitative measures, they feel the results effectively guide their mitigation and prioritization techniques. And there are some security programs who believe quantitative assessments provide specific guidance that determines dollar amount impact in terms of risk.

Quantitative Risk Assessment



The value of either approach is around how results are leveraged to track progress, make improvements, and address remediation, along with how to extract the appropriate content to educate non-technical audiences (i.e. business executives and board members). Results from both assessments provide results that are easily digestible – typically appearing in straightforward heatmaps or graphs.

Some organizations use a combination of both assessment approaches to determine their risk levels, thereby taking advantage of both benefits. Usually, qualitative assessments are the best starting point, they provide a baseline level of understanding around risk and give high-level results. These require internal staff to provide their opinions, getting them involved in the process and hearing directly from team members. Once the fundamentals of a qualitative risk assessment are accomplished, many security professionals explore the quantitative approach. This approach removes the potential for biased results and gives more tangible, business-aligned results. Below are highlights for each approach along with sample results graphs.

Quantitative Assessments

Quantitative risk assessments are a well-defined model that evaluates and measures risk in dollars and probability. It enables organizations to prioritize risk based on economic values and the potential financial impact.

Quantitative Benefits:

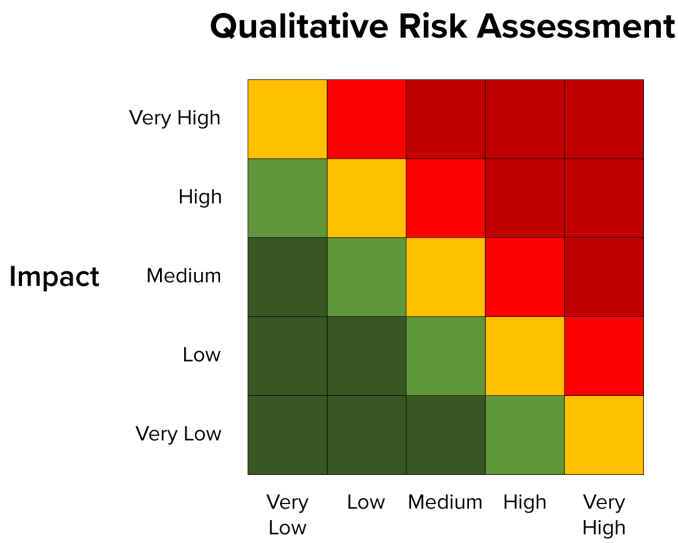
- Leverages factual data measured mathematically or computationally
- Risk is demonstrated in monetary terms and overall financial loss
- Values may include single loss expectancy (SLE), annual rate of occurrence (ARO), and annual loss expectancy (ALE)
- Provides precise values easily understood by business leaders
- Determines impact of risk and resources required to remediate
- Results are consistent regardless of who is performing the assessment (no internal bias)

Qualitative Assessments

Qualitative risk analysis is inherently subjective, solely based on the opinions of the person conducting the assessment. Results are typically based on 1-5 scoring or high-medium-low scales. Results are ideal for security teams who want to provide executives with a high-level overview of risk, displayed in a straight-forward color coded heatmap.

Qualitative Benefits:

- Uses rating scales to determine risk based on frequency and impact
- Represents the relative severity of relative risks
- Based on an individual's perceived likelihood of risks
- Gauges impact on organization's reputation, finance and other factors
- Risks are given numerical values that are easy to work with
- Easy to communicate with simple heatmaps
- Opinion-based so may include biases of people who contribute
- May be limited to internal processes



- May be a tendency to inflate risk – if a risk is between yellow and red they may go with red to be sure the risk is covered

In conclusion, both are great approaches and teams are able to mix and match components of each based on what aligns best with their organization. In security, there is never a one size fits all answer to specific challenges, CISOs and their teams continue to have dynamic approaches, by meeting the needs of the business and addressing risk in a comprehensive manner.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

ASSESSING RISK

FEATS OF STRENGTH
SEPTEMBER 2022