FEATS OF STRENGTH

A BUSINESS-FOCUSED CYBERSECURITY MAGAZINE

CYBERSECURITY BUDGETS

Interviews in this issue:

DECEMBER 2021
KLOGIXSECURITY.COM
617.860.6485

K logix

FEATS OF STRENGTH

CYBERSECURITY BUDGETS

DECEMBER 2021

FROM THE *Editor*

Dear Readers,

As 2021 comes to a close and many security teams are planning for 2022 and beyond, we wanted to focus on the topic of budgets for this issue of the magazine. This continues to be an interesting subject because many CISOs and security leaders we speak with have varying approaches to cybersecurity budgets. They factor in specific priorities within their own teams and the company as a whole, ensuring alignment is ingrained with any initiatives or investments. However, no two approaches or plans for budgets are the same, so we had thoughtful discussions with security leaders to learn more.

Here's what you can find in this issue of the magazine:

On page 4, Aditya Malhotra (CISO, Ness Digital Engineering) discusses how he leverages quantitative metrics and key data points when presenting to boards. He shares his thoughts on gaining justification through demonstrating progress and tips to streamline communication.

On page 6 learn about ways to effectively communicate with executives in order to maintain a healthy cybersecurity budget.

On page 8, Robert Micillo (CISO, MetroPlusHealth) talks about the emphasis he puts on being transparent. He discusses how he is completely clear on where they are today, relative to where they need to be, and some of the dangers of not addressing specific areas of concern.

On page 10, Kelly Haydu (VP Information Security and Technology, CarGurus) thoughtfully shares how she has created strong security awareness and why she ties industry benchmarks to budgetary plans.

On page 12, read research and survey results from reputable sources on cybersecurity budgets. These include if budgets increase or decrease, and what percentage is allocated to security programs.

I want to wish everyone a great end of year and thank you for your continued interest in our magazine!

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

VP Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Manager, K logix

About K logix: Cybersecurity Advisory and Consulting Services

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.

www.klogixsecurity.com/feats-of-strength

Marketing@klogixsecurity.com

ADITYA MALHOTRA

CISO
NESS DIGITAL ENGINEERING

HEADQUARTERS: Teaneck, New Jersey

EMPLOYEES: 3,500+

REVENUE: Private

Aditya Malhotra has dedicated most of his career to information security, working in several leadership roles at enterprises such as Point72 Asset Management and Bloomberg LP. Most notably, Aditya has developed information security teams and built programs from the ground-up, aligned with the firm's business objectives, thereby charting himself as an innovative leader. Currently, he is the CISO at Ness Digital Engineering, a full lifecycle digital transformation firm offering digital advisory through scaled engineering services based out of New Jersey.

Aditya joined the organization four months ago after learning about its vision for growth, emphasis on culture, and overall business model. He saw the opportunity as a way for him to make a meaningful, tangible impact to the organization by bridging the gap between technology, business, and organizational needs. With over 15 years of experience across various facets of information security, Aditya shares his thoughts on the evolving role of CISO responsibilities and advice for leaders in similar functions.

ENGAGING WITH THE BOARD AND EXECUTIVES

Aditya believes security leaders should have direct visibility and involvement with the board to provide insights into key risks and granular visibility of the inherent versus residual risk portfolio across the entire enterprise. He says, "Security leadership has a birds' eye view on the enterprise threat landscape. They have the foremost ability to convey risk and potential impact to the organization in a language board members will understand and be receptive to."

Aditya encourages CISOs to be armed with quantitative metrics and key data points when presenting to boards. He explains, "Metrics help us understand the key areas of risks that the firm is facing today, and which of those risks require action based on criticality and priority. Managing those risks often requires investment in technology and getting additional resources, whether it's external, internal, or contingent workers. So, we are uniquely positioned to provide stakeholders visibility on the intricate nuances of enterprise risks and mechanisms to mitigate some of the major identified gaps. And that's why it is pertinent for security leaders to have a seat at the board level."

Aditya recommends explaining intricate technical nuances in simplistic terms through visual representations such as charts, graphs, or heat maps so the audience can easily ingest the material and then make an informed decision. He sees value in demonstrating different types of metrics for various stakeholders. He says, "For example, the technology leadership and the CIO function should get a different level of visibility and granularity compared to the board. Talking specifically about the board, for example, if I'm looking at our perimeter protection, the leaders would be interested in learning the different types of threats (spear phishing, malware, ransomware attacks) that are being prevented but more so interested in the ones that are circumventing our existing controls."

He continues, "An example of leveraging metrics would be when discussing a Single Sign On (SSO) solution. We cannot expect end-users to remember credentials for tens and hundreds of applications they have access to daily. Eventually, users will end up reusing the same credentials across multiple applications or storing the credentials insecurely, posing a risk for the enterprise. By implementing an SSO solution, I eliminate the need for the end-user to remember credentials for each application. In addition, when

an end-user is terminated, we disconnect one credential and not concerned about the myriad of applications the end-user has access to. These granular metrics demarcate actual data for mitigating risk and building a cohesive risk management culture across the firm. Talking about metrics, it is vital to convey the message in simple terms and give executives business-centric examples that they can understand, connect, and relate to. I feel this is the best way for leadership to grasp the content and get their support on key initiatives."

Aditya says that once you have identified the gaps, made a case for the investment, received budget approval, and implemented the solution, you need to demonstrate cyber security program maturity based on quantitative metrics that are hard to refute. According to him, risk management is a continuous process. Monitoring the current state and demarcating progress towards a future desired state in quantitative terms bridges the challenges we have experienced with rationalizing budget allocations based on qualitative metrics over the years.

BUDGET JUSTIFICATION FOR HIRING

When it comes to adding additional headcount, Aditya says it comes down to prioritizing the initiatives based on business objectives and defining a timeline to complete them. He explains, "Since I've joined, I've identified several initiatives that would assist towards building and maturing the cyber security and risk management program. Obviously, some of them are process enhancements that are easier to accomplish by bringing leaders across the enterprise together. However, others, such as maturing an Identity and Access Management (IAM) function, require dedicated personnel. Making a business case of why we need to mature an IAM program is easy. However, a tricky proposition is when you talk about why you would want to build the skillset in-house for certain programs where others can be outsourced. The decision to build the function internally versus getting support from external vendors should be adjudged based on the execution priority of the initiatives and the time to value. As I'm working towards expanding my team, my pragmatic rationale is driven by initiatives that directly correlate with business operations and their timely execution. And for that, you need resources."

Aditya adds that seeking buy-in from the CFO, CEO, and board is vital for the initiatives to succeed. When he is pitching a business case for specific initiatives, he discusses the technology or toolset investments required and resources needed to ensure the solution does not remain a standalone product but is embedded in the firm's DNA across the entire technology and business verticals. This would require building the business and technical skills in-house and ensuring the program matures over time to support and augment business operations.

He comments, "I'm a big advocate of hiring/working with people across departments who are self-driven, motivated and have a hunger to learn this ever-expanding cyber security space. This means there could be resources and advocates in other departments and functions whom I can collaborate with while working towards initiatives that demonstrate tangible progress and improvement towards risk management."

RESPONSIBILITIES AND GOALS

Aditya is responsible for cybersecurity, data protection and overall risk management across the enterprise and has identified short, medium, and long-term goals. These include implementing a comprehensive security awareness training program with phishing simulation exercises for all employees. He comments, "The main goal is to define a baseline of the risk landscape when it comes to security awareness for employees by imparting phishing simulation exercises. This will help us identify users and departments that need further proactive training to detect and thwart sophisticated threats such as spear phishing."

He is progressing towards onboarding a scalable cloud solution and provides multi-language capabilities for employees across the globe. He continues, "I'm also enhancing the vulnerability threat management program for the firm, which will involve a structured process of identifying vulnerabilities, classifying them, and proactively mitigating risks by adding compensating controls in addition to timely patching and threat remediation."

Building a Governance, Risk & Compliance (GRC) program is also a top priority to manage the multitude of third-party vendors and clients. By structuring that process, Aditya and his team will provide additional layers of visibility. The governance function manages various components of information security such as policies, procedures, standards, insider threat detection, response, third party vendor risk management and mapping of controls to established frameworks. Building a robust information security program requires support from leaders across the enterprise. As each initiative is immersed in the firm's culture, slowly and steadily, you realize a positive cultural shift towards proactive risk management. He says, "Risk management is driven by firm's risk tolerance and reducing risk to an acceptable level."

Lastly, since the organization has a significant presence in Europe, Asia and North America, a large part of his responsibility is reviewing data protection, privacy directives with legal for onboarding new clients. Like many CISOs who are now responsible for data privacy concerns, Aditya continually works towards GDPR alignment. He says this is vital to confidently tell customers their data is safe and secured if an incident does occur.

Aditya says his initiatives towards building a mature cyber security program requires constant reinforcement of foundational cyber security best practices. He explains, "The most important piece for any organization is to know what assets we have. With the growing advent of cloud applications and infrastructure, answering this basic question can be quite challenging. Understanding where all our assets are, data and how to prioritize the protection of data based on asset, data criticality and classification is key. These basic tenets should be embedded in the firm's culture, which will assist in building a proactive risk management function."

Aditya says he is driven to empower and uplift his team and continuously focuses on identifying ways to enhance the team's development and unlock their true potential. He prefers to hire people with a strong affinity for problem-solving and critical thinking. He adds, "As long as I can find a rough diamond who is eager to learn and ready to face new unknown challenges each day, I can polish them over time to carve out their true potential."

Personally, Aditya believes in continuous learning and holds a Master of Science in Information Security from Carnegie Mellon University. In addition, he has several cyber security and ethical hacking certifications. He often leverages his professional network to brainstorm upcoming cyber security challenges.

BUDGETS:
TAKING A PROACTIVE APPROACH TO CYBERSECURITY BUDGETS

By Katie Haug (K logix)

When we speak with CISOs, it is evident there is not a one size fits all approach to cybersecurity budget planning. There is also no golden standard for how much should be spent on cybersecurity each year. From our conversations with security leaders, these are the top variables impacting cybersecurity spending and budgeting:

1. Company vision for innovation and growth
2. Executive and board support of cybersecurity initiatives
3. Industry
4. If the company is publicly traded
5. Compliance and regulatory requirements
6. Overall IT budget
7. Any planned organizational changes

BUDGET DISCUSSIONS START WITH COMMUNICATION AND EDUCATION

From our extensive research, we have found that before budget discussions begin, security leaders should ensure they have a strong foundation of communication between themselves and the business leaders within the organization, from each executive to board members.

Communication should be two-way and include education about the value of security and how security may positively impact each department within an organization. By educating business leaders and executives, they feel ownership for the overall security of the company. They gain a sense of investment in ensuring the company remains secure and that they are an active participant in protecting valuable customer and employee data. Once clear and open lines of communication are established, budget discussions become more transparent.

On page 10 of this magazine, Kelly Haydu (Vice President of Information Security and Technology, CarGurus) says, “A lot of times employees might not understand how security ties back to their work or their function. If you can start to talk about how that ties back to the strategic initiatives or the products or programs that they’re running, you’ll get better buy-in. You must form the relationships through something like a roadshow. People that are solely focused on the technology will sometimes fail in that area because they haven’t been able to socialize why their function is important and how it relates to the other business units. So, getting that roadshow going and meeting with other stakeholders is important. Be careful not to give too much information to people in your first meeting, though. Security can be overwhelming to those that have had little

to no exposure to it."

The CISOs we spoke with said these are the best approaches to strengthening communication with executives during budget discussions:

1. Use business language
2. Provide clear justification
3. Demonstrate the positive impact of security initiatives
4. Discuss simple metrics correlated to business goals
5. Prepare to share progress and ROI

ALIGNMENT WITH STRATEGY

Taking a proactive approach to setting cybersecurity budgets requires clear alignment with the organization's strategy to predict and prepare for any budgetary needs. Many security programs get caught up in the unfortunate cycle of putting out fires and often lack the ability to cohesively drive an established budget plan.

While there always tends to be reactive budgetary spend in security to some degree, security leaders who anticipate this, are able to bake it into their budgets. It starts with creating a strong strategy and roadmap, one that identifies areas of strength and weakness, then delineates investments based on a prioritized list.

On page 8, Robert Micillo (CISO, MetroPlusHealth) says, "I think that the most important thing that I've done is to provide the executive team complete transparency. I don't sugarcoat anything. I'm a very transparent person. I want to be completely clear on where we are today, relative to where we need to be, and what some of the dangers are by not addressing specific areas of concern. The aim is to reduce risk to an acceptable level to prevent a breach, so when presenting cost benefit analysis it is often weighed against the cost of breach potential. When you talk about a breach, we need to be cognizant of several things that people don't easily see. Reputational damage within the industry and fines are top of mind, but what you may not recognize are the costs involved well beyond the framework of government fines. There are residual mitigation costs and consider public confidence—the minute you lose public confidence, you're losing membership."

ROBERT MICILLO

CISO
MetroPlusHealth

HEADQUARTERS: New York, NY

EMPLOYEES: 1,500

REVENUE: $3.7 Billion

Robert Micillo has over twenty years of experience working in the healthcare industry, which prepared him well for his role at MetroPlusHealth providing quality, affordable health insurance benefits to over 625,000 New Yorkers. He says, “When I was being interviewed, it was apparent that although they had security measures in place, they needed someone who could come in to create and implement a more comprehensive security program that met all the new, emerging regulations. It became a very natural conversation as I was able to map out for them a security program that fit their needs.”

Micillo’s core responsibility when joining MetroPlusHealth was to define an information security program in order to reduce risk, protect the organization, meet regulatory requirements, and safeguard membership data. By establishing a strong, comprehensive approach to security, he ensured goals would be met and the organization would be positively impacted by the growth of the security program. Initially, Micillo completed a risk-based assessment of their current security posture and tools, worked to rewrite their policies, completed a staff assessment to map out the positions and requirements to put together a team, and defined and delineated roles between information security and technology support.

His goal from the onset was to provide the necessary means to protect the assets and data, while maintaining operational efficiencies. He explains, “The MetroPlusHealth Cybersecurity program must strike the right amount of security measures to protect customer privacy and our assets while ensuring operational efficiencies for our business units. It’s kind of a balancing act, because I can add security measures that can lock down things so tightly that we start losing operational efficiency and vice versa. We may gain so much operational efficiency that we lose track of maintaining and securing our digital assets. So, I find it to be a true balancing act, and we do it fairly well.”

CORE RESPONSIBILITIES

Micillo has six program areas covered by his department – security operations, risk management, security awareness and training, business continuity, policy and governance, and security architecting and engineering.

Security Operations – The security operations team focuses on having 24/7 visibility. Micillo says, “We’re pulling in as many raw logs as we can from as many sources as we are able to, to identify anomalies, to identify brute force attacks, to recognize whether what we’re seeing is real, or an anomaly, acceptable and expected behavior or a false positive.”

Risk Management – He explains, “From a risk management perspective we’re monitoring and assessing technical and

operational risk regularly. We're currently focusing on, and this is very important, evaluating and measuring third-party risk. We share our data with a lot of business associates out there, and we are able to do some degree of due diligence and monitoring on what those third parties do for us, how they handle our data, and what the propensity of their security program looks like. We want to identify if they maintain a strong, medium, or low security posture over time through increased visibility into their security practices." This is an area of focused concentration in the third-party risk management roadmap for the organization.

Security Awareness and Training – Miccilo and his team focus on security awareness and education across the MetroPlusHealth staff in order to minimize risk. He acknowledges that their employees are the first line of defense in many cases and an integral part of maintaining good security habits. Ultimately Micillo acknowledges they are only as strong as their weakest behavior and therefore allocate ample resources on training and education, and provide employees with a simple and easy way to report suspicious activity.

Business Continuity – They have a comprehensive business continuity program where they work with the organization's units to identify their tolerance levels. Micillo continues, "Depending on the interruption of business, we want to identify what the next best move would be and how it would be triggered. And we put all those plans together for the departments as a whole. I have a dedicated team who gathers that intelligence and understands the RTO and RPO requirements behind what their needs are to maintain business and keep the wheels of motion going."

Policy and Governance – Micillo comments, "It's always my goal to separate policies from procedure. Procedures can contain steps that may change rapidly based on new standards while policies should not change that quickly or easily, and should be amended based on requirements from regulator and compliance sources. So there's a lot of work that goes into policy development. And the key to good policy is obviously one that employees can understand and meet. We strive to ensure that our policies are meeting compliance, are comprehensible, achievable and that they're not so stringent that we cannot comply with them."

Security Architecture & Engineering – Security team members are dedicated to innovative initiatives taking place within the organization to make sure they are secure. Robert says, "API management is a very hot topic right now as we're going through a lot of transformation, and that requires a specific technical strength that I don't find in every engineer that I run across. That onto itself is a very important piece of the puzzle here."

TRANSPARENCY WITH EXECUTIVES TO JUSTIFY BUDGET

"I think that the most important thing that I've done is to provide the executive team complete transparency. I don't sugarcoat anything. I'm a very transparent person. I want to be completely clear on where we are today, relative to where we need to be, and what some of the dangers are by not addressing specific areas of concern. The aim is to reduce risk to an acceptable level to prevent a breach, so when presenting cost benefit analysis it is often weighed against the cost of breach potential. When you talk about a breach, we need to be cognizant of several things that people don't easily see. Reputational damage within the industry and fines are top of mind, but what you may not recognize are the costs involved well beyond the framework of government fines. There are residual mitigation costs and consider public confidence—the minute you lose public confidence, you're losing membership," says Micillo.

He believes in bringing these important issues to the forefront because if you are not able to make them apparent, budget decision makers may not express buy-in with your decisioning. When he first started, Micillo outlined 30-to-40 initiatives he believed the security program needed to accomplish within one year, something which is often unprecedented in the security realm, especially with compliance requirements and regulations that drive organizational decisions.

He explains, "I came in with a plan. If you don't have a plan to create a program that can identify all of these things, I think it becomes that much more difficult to justify the funding. I think that I was able to accomplish it. I was very fortunate because I really understand the business and the dilemma that MetroPlusHealth was facing at the time. And the stars aligned from that perspective that I was in the right place at the right time for the right situation. And I'll tell you, I think that we have an extraordinarily strong program. I know for a fact that the Board of Directors and the CEO are extremely proud of what we've accomplished. I've only been with MetroPlusHealth since 2017 and that's not a long time to put something together that is this formidable and I'm very proud of it."

KELLY HAYDU

Vice President of Information Security and Technology
CarGurus

HEADQUARTERS: Cambridge, MA

EMPLOYEES: 900+

REVENUE: $551.45 Million

When Kelly Haydu was asked by a recruiter to take a meeting with CarGurus's CTO, she initially went into it thinking it would be a good networking opportunity, however once she learned more about the organization, she knew it would be a great fit for her career. Kelly says, "I really wanted to understand, what was their vision, what was their strategy? Is it a place that I would want to work? I talked to many individuals and with every conversation I was impressed with their culture; the people were just outstanding. Everyone I spoke with was genuine and wanted to do the right thing. Integrity is a core value of CarGurus which is important to me. I knew it was a place I could be happy."

She continues, "CarGurus has such a great group of people. Leaders in security roles aren't always welcomed to the table. They have invited me with open arms. I am grateful for that and the executive support I've received."

CarGurus is an automotive research and shopping website that assists users in comparing local listings for used and new cars and contacting sellers. As an innovative, rapidly growing company, Kelly says that during initial conversations it was clear the organization recognized the importance of a mature security program. With new digital tools and additional transactional capabilities including their Instant Max Cash Offer (IMCO) and the acquisition of CarOffer, ensuring seamless and robust security was a necessity. Kelly comments, "I think the company understood that in order to expand beyond a listings business, they were going to need additional security around those existing and new product features."

Before her tenure in the security space, Kelly worked in Quality Assurance including lead automation roles across markets and verticals. She served in various previous roles as Director and Senior Director in Information Security prior to taking on the Vice President of Information Security role at CarGurus. In August of 2021, IT was brought under her department, and she became the Vice President of Information Security and Technology.

CREATING STRONG SECURITY AWARENESS

Kelly's first and foremost responsibility is to educate all employees about their responsibility to the overall security of the organization. Creating a strong awareness and educating the workforce is key for her to ensure security is baked into their everyday culture. She explains, "Creating awareness and education across the whole employee base is really important. Once people start to understand what those security best practices are, I often hear them say they had an 'aha' moment when they're working in their particular department and they're handling personal data or they're handling confidential data, or they get an email and they're not sure if they should click on that link. It causes people to think about security in a different way and to sometimes pause. My job is to educate, but also to make

sure that you get to a point where employees carry those best practices into their personal lives."

The security program under Kelly includes risk & compliance, application security and security operations. IT remains as a separate department but both teams work closely together. By focusing on these core areas, Kelly comprehensively focuses on both risk reduction and increasing security maturity.

Under risk and compliance, the security team focuses on streamlining the vendor risk assessment process to enable the business to move quickly while still gaining visibility across vendors and partners. For their security team, understanding security risks and evaluating them has been a large project, which goes hand in hand with understanding all end user applications they use on their machines.

For application security, Kelly and her team focus on the Software Development Lifecycle (SDLC) process and how they can instill the 'shift left' mentality and approach. She explains, "We've tried to build security architecture reviews into our SDLC process. We are still building the program. We want to make sure that we are providing recommendations for secure coding and collecting feedback from the product and engineering teams. It is important for the application security team to gain insights earlier into that review cycle when the ideas are incubated to understand what are the necessary security protocols and what are the risks."

One of the biggest focus areas for security operations is around automation. Kelly says they have already started building a golden AMI pipeline so they can hone-in and have an automated strategy for patching their infrastructure systems. Her background working as an automation engineer has provided her ample exposure to ensure their automation goals are met.

The IT program is in the process of hiring an Identity & Access Management engineer to help orchestrate identity solutions across the entire organization. This involves a deep understanding of what they have today in order to streamline and consolidate to avoid redundancy of multiple systems.

INDUSTRY BENCHMARKS AND TYING BUDGET TO THE BUSINESS

When planning and strategizing for budgeting, Kelly recommends reaching out to your network of CISOs to better understand how to approach this sometimes daunting task. Kelly states, "My advice would be if you're going to go out and do an industry benchmark, make sure that you're benchmarking against your industry, including public and private companies. That is important for not only where you are today, but if you're a growth company, where you're going to go. You must make sure you are telling the story and showing them the picture of where we you are and what the risks are to your business."

"A lot of times employees might not understand how security ties back to their work or their function. If you can start to talk about how that ties back to the strategic initiatives or the products or programs that they're running, you'll get better buy-in."

By getting ahead of the curve and demonstrating the long-term benefits of having the appropriate staff and budget, you avoid playing catch up or being behind. Kelly says what is key to remember is tying it back to business and strategic initiatives to exemplify how security provides value to the organization.

According to Kelly, conversations with executives about budget are most successful when CISOs have invested time in educating the business about the importance of security. She suggests putting a roadshow together that includes roadmaps with major initiatives or projects and to get in front of each business unit to show them what the security team plans to accomplish. She explains, "A lot of times employees might not understand how security ties back to their work or their function. If you can start to talk about how that ties back to the strategic initiatives or the products or programs that they're running, you'll get better buy-in. You must form the relationships through something like a roadshow. People that are solely focused on the technology will sometimes fail in that area because they haven't been able to socialize why their function is important and how it relates to the other business units. So, getting that roadshow going and meeting with other stakeholders is important. Be careful not to give too much information to people in your first meeting, though. Security can be overwhelming to those that have had little to no exposure to it."

CYBERSECURITY BUDGETS: BY THE NUMBERS

RESEARCH FROM K LOGIX AND OTHER REPUTABLE SOURCES

By Katie Haug (K logix)

Since no two cybersecurity budgets are the same, we conducted research across the industry to better understand typical budgets. There are a number of reputable studies that shine some light on recent budget trends.

WILL BUDGETS INCREASE OR DECREASE?

K logix conducted a study with over 200 CISOs across all verticals and the results showed us that 42% said their budget increases 5-10% per year, 48% said it remains around the same and 10% said it is expected to decrease.

We are able to dive deeper into our data to reveal results for specific verticals. For example, when we polled CISOs at financial services organizations, almost 50% said their budget increases at least 5% per year. Manufacturing was similar, with 48% saying their budgets increase 5% per year.

ISACA's State of Cybersecurity 2019 report (*State of Cybersecurity 2019; ISACA Cybersecurity Nexus)* states that 12% of survey respondents said their budgets are expected to decrease, 34% said it will stay the same and 55% said it would increase. These results track with those collected by K logix, and we anticipate moving into 2021, budgets will continue to increase for over 50% of organizations.

ESG recently published its annual IT spending intentions research for 2020 *(2020 Technology Spending Intentions Survey*; Enterprise Strategy Group Research) and found 55% of organizations planned to increase overall IT spending in 2020. At least half of organizations in the health care, technology, retail/ wholesale, manufacturing, and business services industries will increase IT spending in 2020.

The 2021 CIO Pandemic Business Impact study (*Spring 2021: State of the CIO*; CIO from IDG) states that to drive business forward, 50% of IT decision-makers anticipate that their tech budgets will increase over the next 12 months, 42% anticipate their budgets will remain the same, and only 8% expect a budget decrease – which is in line with the 7% in December 2019 prior to the pandemic.

From these surveys and the ample amount of available research on the topic, it is clear that over 40% of security programs anticipate increased budgets in the next 12 months. The amount of increase does differ company to company, and it is often driven by variables such as corporate plans for growth, compliance requirements, etc.

Organizations are investing more in their cybersecurity programs because they see the importance of protecting valuable assets that impact both employees and

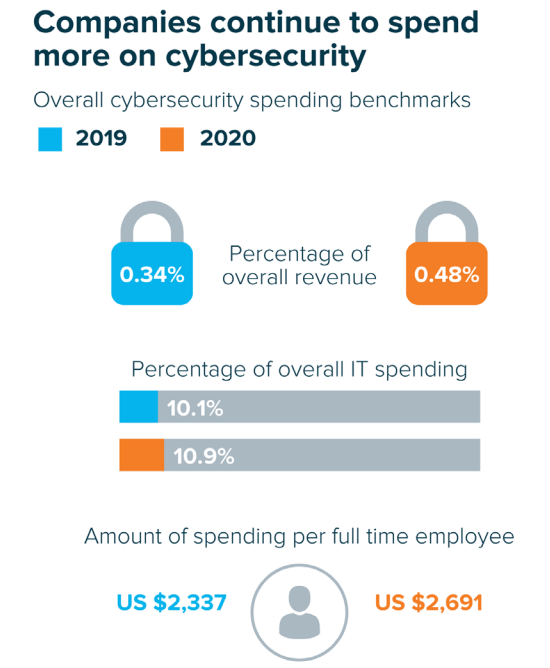

Image Source: (FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO Survey Reports; 2019 and 2020; Deloitte Center for Financial Services analysis)

customers. By continuing to invest in cybersecurity, there is an opportunity to protect company-wide innovation and growth.

WHAT % OF THE IT BUDGET IS SPENT ON CYBER?

According to a study released by Deloitte (*FS-ISAC/Deloitte Cyber & Strategic Risk Services CISO Survey Reports*; 2019 and 2020; Deloitte Center for Financial Services analysis) the average company will spend somewhere between 6% and 14% of their annual IT budget on cybersecurity.

They found that on average, most companies spent around 10% of their IT budget.

In the study results, the average spend per year per employee is:

Financial Utility: $4375 per year per employee

Service Providers: $3266 per year per employee

Banking: $2688 per year per employee

Consumer/Financial (nonbanking): $2348 per year per employee

Insurance: $1984 per year per employee

The Deloitte study, among others we found all point to companies continuing to spend more on cybersecurity.

Based on an IDG survey (*2019 Security Priorities Study*; IDG Communications) of 664 security-focused professionals worldwide, nearly two-thirds of enterprises (60%) plan to increase security budgets in the next year, by an average of 13%. This number is on the high-end of the research we found, but exemplifies the investment organizations are willing to make in order to increase maturity and overall protection.

CIO's 2019 State of the CIO survey (*2019 State of the CIO*; CIO from IDG) revealed that on average, 15% of a company's total IT budget was dedicated to IT security. This is slightly higher than the other studies, but still tracks within the 1-15% range.

CONCLUSION

The majority of organizations (almost 50%) say their budgets increase on a yearly basis. While there are a number of determining factors for this, we found the most common responses to why their budget increases to include:

- Stronger alignment between security leaders and the business
- Rising threats including an uptick in ransomware
- Protecting innovation and growth initiatives
- Increased awareness of cybersecurity across an organization
- Compliance and regulatory mandates

From our research, the average organization spends 10% of their IT budget on cybersecurity. The variables that impact this percentage include company size, industry, among many other factors.

We have found most business leaders are keenly aware of the value of investing in security programs. They see direct correlation between protecting the organization and the positive results by doing so. Strong security programs that are continually reducing risk and increasing maturity ensure the on-going protection of customers and employees.

Only some CISOs we speak with struggle to demonstrate the ROI or competitive advantage of security programs; the majority of CISOs are in a mature place where they can measure and demonstrate progress. Those who are able to show progress and justification for budgetary spend typically receive increased budgets year-over-year.

Overall, we believe security is becoming ingrained in organization culture through stronger communication and transparency with business leaders.

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

K logix

CYBERSECURITY BUDGETS

FEATS OF STRENGTH
DECEMBER 2021