FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

SECURITY BUDGETS

FOCUS ON JUSTIFICATION

IN THIS ISSUE:

DECEMBER 2022 KLOGIXSECURITY.COM 617.860.6485

TABLE OF CONTENTS

Budgets *December 2022*

FROM THE *Editor*

Dear Readers,

For the second year in a row, we are focusing on cybersecurity budgets in our December issue of Feats of Strength magazine. Budgeting continues to be at the forefront of security priorities and conversations with executives and the board, yet many security leaders feel they have limited resources to help guide their approach to budgets.

We consistently hear from the CISO community that there is no one size fits all approach to budgets, however they all share the importance of justifying security spend by demonstrating impact to the business. This could be in the form of metrics such as a risk quantification model or clear return on investment numbers. Or to focus on the value of preventing losses due to cyber-attacks.

In this issue, we spoke with nine CISOs/security leaders who shared their advice, thoughts and experience with cybersecurity budgets.

Page 4: We profile Alan Berry, CISO at Centene Corporation. Alan brings cybersecurity experience from his 26 years in the Air Force and shares his approach on leading security for 82,000+ employees.

Page 6: Read our Q&A article about cybersecurity budgets, including responses from seven CISOs who share their direct experience and thoughts on pertinent topics.

Page 10: We profile Matthew Mudry, CISO at HomeServe North America. Matthew discusses his approach to cloud transformation, how to efficiently connect with the business, and why he leads his team by example.

Page 12: We include an article about cybersecurity budgets and how to take a proactive approach. Learn specific numbers, percentages, and break downs of typical budgets.

Something to think about in the context of the economy is the current state of inflation and how it impacts budgets, and causes unpredictability. When inflation starts going down, what will the impact to cybersecurity budgets be? How will the way security programs use resources and spend money change? How will it impact maturity? I'm interested in hearing the thoughts of our community members as this story continues to develop.

We hope you enjoy reading!

Kevin West

CEO, K logix

Magazine Contributors

Katie Haug - Editor
VP Marketing, K logix

Kevin West - Editor
CEO, K logix

Emily Graumann - Graphics
Graphic Designer, 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*

ALAN BERRY

CISO
CENTENE CORPORATION

HEADQUARTERS: ST. LOUIS, MO

EMPLOYEES: 82,400

REVENUE: $125 Billion ($142 Billion projected for 2022)

Before becoming a CISO, Alan Berry spent the first 26 years of his career in the Air Force, where he worked across multiple departments and positions. His roles included the Director of Communications (CIO) for Air Forces Central, Commander of the 624th Operations Center (the command and control center for the Air Force global networks) and the Chief of Staff for Air Forces Cyber at Fort Meade in Maryland.

Although his work varied over the course of his 26 years in the Air Force, he found himself always coming back to work in cyber security related roles, positioning him well for the next phase of his career. After leaving the Air Force, Alan took on the role of Senior Director of the Disaster Recovery team at CVS Health where his work included restructuring the teams and technologies involved with disaster response.

After leaving CVS in 2017, Alan began working at Centene Corporation, the largest Medicaid managed care organization in the country. Centene provides a portfolio of services to government sponsored healthcare programs. He was initially hired as Vice President of Cyber Security and after three years transitioned into the CISO role.

Alan explains, "I was originally hired to lead all security operations, crisis management and business continuity. At the time we didn't have a CISO, and the job had been divided up into three people, me being one of them, but two years ago we decided to move back to having one traditional CISO role, which combined all of those responsibilities back into one office under one person."

Joining Centene was an easy choice for Alan because he believes in the organization's core mission. When he worked in the Air Force, Alan's job was to protect and defend whatever mission he was responsible for, ranging from space operations to transportation, refueling, and combat missions across the globe. He was committed to defending these areas from a cyber perspective so adversaries could not impede the ability to conduct the missions. Alan explains, "It's the same thing a CISO does, and it's very easy to protect honorable missions. Centene works in government healthcare, providing healthcare to people who wouldn't otherwise be insured. Our mission is to transform the health of the community one person at a time. It's easy for me to get up every morning and commit to helping Centene's mission."

CORE RESPONSIBILITIES AS CISO

Alan's responsibilities include all security operations, and incident response including threat intelligence, adversary hunting teams, and detection engineering. He oversees all systems that support these areas such as firewall proxies, vulnerability management scanners, email security systems and other key functions. His team also owns the identity process from ensuring new employees are properly entitled to managing single sign on, multifactor authentication, and everything in between.

"Our mission is to transform the health of the community one person at a time. It's easy for me to get up every morning and commit to helping Centene's mission."

They also manage cloud transformation as it relates to security.

As the organization continues to transition to the cloud, Alan and his team ensure security is top of mind and transforming at the same pace as the business. Alan comments, "I'm focused on increasing cyber resiliency in this cloud transition process. Moving security tools to true cloud platforms, and still performing the same functions should gain resiliency out of that. But if we don't go into it with purposeful intent, then we likely won't improve anything. There is a lot of focus to make sure what is moved to the cloud actually gains resiliency."

COMMUNICATING EFFECTIVELY AND PROACTIVELY

Alan's tenure in the Air Force prepared him to focus on communicating effectively and proactively with executives and the board. While in the Air Force, he had to translate between mission owners like pilots, and the technical team working to fulfill the mission itself. He says, "I had to learn how to speak like a pilot or mission owner and translate the work I was doing into their language. Translating operational imperatives in the military world is no different than doing so in the corporate world. It is the same thing in a government-specific medical insurance organization, there is very specific language used on a daily basis and I have to be able to speak the language of the business to be successful."

By speaking the nuanced language of the industry Alan works in, he is able to both partner with the business and translate anything back to his team to take action on. This positions him for success, as he avoids siloes and focuses on continually unifying security with business priorities.

He explains, "For the security industry, ten years ago it was a different story with security and the business. It has improved significantly. As executives have learned more about the business of security, they have gained an appreciation for the value security brings, and discussions have become easier for security leaders. Especially as boards see incidents and other newsworthy security events happening at peer organizations. Today, most executives are invested in what security is doing and believe in what we all do enough to help us do it even better."

AN INTENTIONAL APPROACH TO TEAM LEADING

Alan has adopted what he calls an intentional manner when communicating. He comments, "I can be very directive in how I communicate, so it's important for me to consult with team members instead of deciding actions for them. I don't want to download the answer for anyone, I have learned to intentionally stop myself and ask them their thoughts. I enjoy when my team builds their own answer or response, and I am able to represent it for them."

When dealing with conflicting opinions, Alan relies on guiding team members through the issue by clearly laying out the pros and cons. Instead of trying to prove a case, Alan believes in taking a step back and thinking through the other person's approach and thought process. By identifying the driver of the other person's position, Alan better understands how to communicate and resolve any issues.

Alan also strongly believes in education for his team. He comments, "We have made an overt effort to focus on our internal employees' careers and education. We use NIST's National Initiative for Cybersecurity Education (NICE) framework which clearly spells out roles in cyber. We took all of these roles and turned them into Centene roles. We put in preferred education around those roles, including any certifications or additional education that is desired. This way, teammates can look at the career ladder and understand their options for growth. It helps them prepare for roles they want to grow into, and what education they might need to get there."

API SECURITY, GOING PASSWORDLESS AND CLEARING THE ZERO TRUST NOISE

When looking ahead in the cyber industry, Alan says understanding API security will be critical for security leaders. With more systems, platforms and vendors in the cloud space, and data being exchanged in real time through APIs, security professionals must retain a strong knowledge of how this works and the impact to their programs.

Another area of focus for the industry is going passwordless. Alan believes it will transition to more mainstream and eventually become a common approach for many organizations as the complexity of passwords increases.

The other trend Alan has noticed is that organizations are moving past the buzzword filled Zero Trust marketspace. He says, "We can finally get down to the brass tacks of what companies can do in the Zero Trust space. It has been a challenge in previous years and sometimes the noise is hard to get through to understand what Zero Trust means for your organization."

CISO Q&A

CYBERSECURITY BUDGET QUESTIONS ANSWERED

By Katie Haug

We asked budget questions to our community of Feats of Strength CISOs. These include CISOs who were previously featured in the magazine and have continued to contribute on a regular basis.

These experts share their thoughts on hot topic budget areas such as justification, focus areas, and more. The benefit of hearing directly from CISOs is learning from their past experiences when dealing with cybersecurity budgets and how they approach resource distribution and spend. As one of the more challenging areas that security leaders are responsible for, the more we hear from our network of CISO peers, the better informed our community will be.

The security leaders who contributed to this Q&A include:

Bradley Schaufenbuel
VP & CISO, Paychex

Rob Sherman
CISO, American Tower

Debby Briggs,
CSO, NETSCOUT

Tim Swope,
CISO, Catholic Health

Doug Graham
Chief Trust Officer, Lionbridge

Tom Meehan
President, ControlTEK

Jon Fredrickson
VP & Chief Risk Officer, BCBS of RI

What are the best ways to justify cybersecurity spending to board and executives?

Bradley Schaufenbuel: I would suggest leveraging an economic risk quantification model such as the Factor Analysis of Information Risk (FAIR) to illustrate unmitigated cyber risk as well as the impact of spending proposals in mitigating those risks in terms of dollars and cents. Finance is the language of business, so I have found that presenting risk and risk mitigation efforts in economic terms resonates better with a senior leadership audience.

Debby Briggs: The best way is to engage with the board and executives in business terms. You need to explain what the risks are to the business, and what are the potential costs of not spending the money. It is always good to know your current IT Security spend as a percentage of IT spending, and as a percentage of revenue, against your peers.

Doug Graham: There needs to be an overarching plan that fits with the business plan and objectives, not just a series of tactical asks. In most cases, executives will ask the question, "what if I don't do this thing" to the extent that you can answer that question you should. For companies that deliver B2B services, it's important to channel the fact that there is an expectation from the customer that certain security measures are in place. When we tie security to revenue, or more appropriately draw the link between having adequate security and not losing revenue it can help to make the case.

Jon Fredrickson: It's in the form of a non-technical business case. It needs to always show an ROI. Either directly (process improvement, user experience, etc.) or indirectly (mitigating a quantified risk).

> *"Finance is the language of business, so I have found that presenting risk and risk mitigation efforts in economic terms resonates better with a senior leadership audience."*
>
> *- Bradley Schaufenbuel, VP & CISO, Paychex*

Timothy Swope: World, national and business area (healthcare, retail, etc) threats and risks that directly affect your industry should drive the need for expenditures to remediate and mitigate those risks. Often, there is a ROI as spending on cyber can reduce cyber insurance cost, litigation for breaches and other negative outcomes of cyber breaches.

Tom Meehan: It's important for organizations to be able to justify cybersecurity spending to board and executives. There are several different ways that this can be accomplished, depending on the particular organization's situation. One way is to focus on the value of preventing losses due to cyber attacks. This can include costs associated with data breach notifications.

What program areas are the most challenging for CISOs to acquire budget for? Why?

Bradley Schaufenbuel: Program areas where it is difficult to estimate and measure the impact of cyber risk reduction efforts are the most challenging to justify. An example of that is an investment in training and developing cyber security professionals. It is difficult (but not impossible) to estimate or measure how much cyber risk is reduced because an employee is better trained.

Debby Briggs: Most challenging is headcount, I know that this is not a program. I think the reason for this is that it is an ongoing cost, that if no longer needed goes against NETSCOUT's philosophy and culture of, "Lean but not Mean".

Doug Graham: In my experience, the softer aspects of managing the security program are the harder things to justify spend on. Things like GRC tools or tools that don't directly reduce risk (like technical tools might) tend to be a harder sell because the value statement is generally softer.

Jon Fredrickson: Emerging threats. Sometimes it can be difficult to convey why our existing tools are not "good enough" for the current situation/threats.

Timothy Swope: Staff - cybersecurity staff are in great demand and are costly. In addition, tools that give proactive cyber attack information are often hard to

show the ROI. Finally, GRC (Governance Risk and Compliance) is difficult as it is not "in the forefront" of cyber news.

What advice would you give to a first time CISO who isn't sure how to spread budget between people, technology, processes, etc.?

Bradley Schaufenbuel: I would suggest investing in people first, followed by processes, followed by technology. Technology is useless if you don't have people to implement and operate it. A process is useless if you don't have people to execute it or technology to facilitate it. As the Target data breach illustrated, you can have plenty of people and fantastic technology, but if you don't have a well-defined process for people to respond to alerts generated by technology, attacks go undetected. And we have all seen shops filled with undeployed or misconfigured technology due to a lack of people and/or processes.

Debby Briggs: My advice is that you need to determine where your greatest risks are. If you don't have people, who is going to provide the training programs, or use the technology? As a general statement, people would have the largest budget.

Doug Graham: I wouldn't advise parsing a budget this way, I'd advocate that CISOs talk to capabilities and understand that there is a people, process and technology underlying most capabilities. We should sell the capability value and price in the necessary people process and technology components – otherwise we risk getting funding for things like tools and not funding for the people to run them.

Jon Fredrickson: Focus on people first, then processes, then technology. Buying tech is much more difficult than attracting and retaining top talent.

Rob Sherman: Make sure you really understand the company and where cybersecurity fits into the business model before deciding where to prioritize your spend. There is no "one size fits all" model to identify where to put your dollars. Second, that old IT adage of people-process-technology also comes into play. Security tools often seem like the best place to prioritize spend. But without the people and processes to implement and respond to alerts, the tools could become shelfware. On the flip side, especially in today's hiring environment, it may not be possible to get the people you need, so that could push to a reliance on additional technology solutions.

> *"There is no "one size fits all" model to identify where to put your dollars."*
>
> *- Rob Sherman, CISO, American Tower*

Timothy Swope: People and training 45%, process 20% and technology 35%.

Tom Meehan: 55% to people, 20% to training, 25% to technology.

What area will CISOs see the biggest budget increase in 2023? Why?

Bradley Schaufenbuel: The areas of largest investment are unique to each organization, as the risks they face and the controls they have in place are different. That said, the areas my peers say they are investing in most in 2023 include zero trust architecture implementations and ransomware prevention and recovery improvements. The reasons for these areas of focus are obvious. Most attacks rely on compromised credentials, making zero trust architecture critical. And ransomware remains one of the most pervasive and disruptive attack types and is growing exponentially.

Debby Briggs: With the talent shortage, and increase in salaries and competition for employees, your people costs will be one of the largest increases. There are technologies like zero-trust and deep packet inspection that will improve our ability to reduce our attack surface and add greater visibility.

Doug Graham: This very much depends on the overall maturity of the program. Frameworks that are based on maturity will naturally drive people to a relative maturity of 3+ on a 5 point scale and where companies are operating below that I would recommend that they spend in this area. Regulatory and legal aspects including privacy will continue to drive spending – they are often the easiest to justify as well.

Jon Fredrickson: Hopefully investing in their people & workforce development. I still think we're in a very competitive job market, so focusing on how to keep your team engaged, trained and sufficiently compensated should be top of mind.

Rob Sherman: 1) Regulatory & compliance given the pending SEC & DHS-CISA requirements 2) Supply chain/3rd party risk management as companies begin to look deeper into their supply chains and realize that there is work to be done to secure those paths into the network.

Timothy Swope: AI tools that give actionable information for operational decisions - these give a proactive cyber posture.

Tom Meehan: In 2023, the area of cybersecurity that will see the biggest budget increase is artificial intelligence (AI). AI-enabled security solutions are increasingly being used by organizations to identify and respond to threats more rapidly and accurately than ever before. As technology advances, so too does the sophistication of cyber threats, making it necessary for companies to invest in AI.

What is your approach to investing money in purchasing new technologies?

Bradley Schaufenbuel: We sort all cyber risks in our enterprise risk register by the amount of unmitigated risk. Where there is a cyber risk with an amount of unmitigated risk that exceeds the appetite established by the board of directors, we search for solutions that mitigate that risk. If that solution is the implementation of a new technology (note: many are not), then we follow a systemic process to set forth requirements for a technology solution, determine which vendors offer solutions that meet those requirements, and then evaluate each vendor's solution via a proof of concept or proof of value. The solution that best meets our requirements at a reasonable cost is selected and implemented.

Debby Briggs: I ask, what are our greatest risks?
Who can we reduce these risks?
What does the threat landscape look like, and does this require me to look to new technologies?
What are the business goals. and how can security support and protect them?

Doug Graham: I like to work with early stage companies that have a direct fit for solving a tactical need. Typically by getting in early I can shape the results to fit and achieve good value for the my program as well as for the technology company – we call these design partnerships.

Jon Fredrickson: The purchasing of new technologies is always last on my list. This will always come after we assess our current toolsets and processes to ensure we can't cover the gap more efficiently.

Timothy Swope: For healthcare - I define the best possible technologies that support patient privacy and safety.

Tom Meehan: When investing in new technology, it is important to look at the long-term benefits of the purchase. It is necessary to consider how this technology will help improve workflows and processes, as well as whether it has potential to increase profits or reduce costs.

> *"When investing in new technology, it is important to look at the long-term benefits of the purchase."*
>
> *- Tom Meehan, CSO & CISO, ControlTEK*

PROFILES IN *Confidence*

MATTHEW MUDRY

CISO
HOMESERVE NORTH AMERICA

HEADQUARTERS: Norwalk, CT (US Headquarters)

EMPLOYEES: 2,500+

REVENUE: $800 Million

Matthew Mudry's interest in technology began at an early age when he started physically building computers, and modifying how the operating systems and applications behaved, to better understand their limits and capabilities. Over time this interest shifted from a hobby into a prosperous career. Today, with over twenty years' experience in IT and security, Matthew continues to be deeply passionate about his work.

Early in his career, Matthew worked in areas such as desktop support engineering, server/storage support, and networking. Matthew's most recent work includes six years at Castleton Commodities International as Vice President of IT Architecture and Security. He helped build a successful security team/program from the ground up, implementing many new technologies and numerous processes and procedures to maintain a safe and secure environment. During this role, Matthew initially oversaw the infrastructure side, with security being a component of that, but the CIO at the time said they were separating infrastructure and building a security team, and asked Matthew to choose which side he would prefer to work on. Matthew explains, "This was about twelve years ago, and without much hesitation, I told him I wanted to switch over to security because I felt it was the right time and I wanted to grow my knowledge in that space. I was excited to go down the security road and that's where my career in security really took off."

Matthew then moved to CareCentix for two years as the Vice President of Information Security. Here, he provided oversight and leadership for both security and networking and was responsible for evolving and maintaining the program, while maintaining HIPAA compliance and working towards and eventually achieving HITRUST certification.

Matthew is currently the CISO at the North American arm of HomeServe, a global provider of home repair and installation services with 4.6 million customers across the US and Canada. He is responsible for the confidentially, integrity and availability of the global systems, the accompanying data and the overall safety of the personnel. His responsibilities include maintaining PCI compliance, continuous improvement to the security posture and integration with newly acquired entities into the business/network.

FOCUSING ON THE CLOUD

As most businesses continue to transform, Matthew's work at HomeServe addresses this trend as they shift to the cloud. He comments, "When it comes to cloud my focus is on securing the data and the systems within it, without jeopardizing its functionality, performance or purpose. The shift to cloud has significantly altered the landscape and changed the way many individuals and businesses approach security. We went from building a number of fortresses, with many layers of security, where all our systems and data sat behind, to securing each individual application and/or creating many smaller secured bubbles so information can be accessed seamlessly and securely from anywhere in the world. The challenge is always around achieving the same level of security, or better, in the cloud without adding too much complexity or impacting its ability to function as expected."

Matthew's approach is to focus more on the endpoint because there are limited protected networks when moving to the cloud. He explains, "To protect your assets, or your crown jewels, whether it's PII, PCI, or other sensitive data, it is important to monitor and manage the endpoint with the least

"When it comes to cloud my focus is on securing the data and the systems within it, without jeopardizing its functionality, performance or purpose. The shift to cloud has significantly altered the landscape and changed the way many individuals and businesses approach security."

amount of impact. Previously you had firewalls, and intrusion detection/prevention systems, network detection and response (NDR) solutions, where you monitor the traffic traversing between the endpoint and your applications/systems, whereas now you need an agent on the endpoint to do all these things. In my mind, it's finding not one product that does it all, but it's finding a few complimentary agents that can solve all these problems."

API security poses a challenge for Matthew because he says with so many different cloud solutions in place, there are often APIs hooking into them, all coming from various locations. He says, "Once in a while you might get an alert, or find a rogue API connection, that was configured by an application owner or system administrator but didn't go through all the necessary channels. Therefore, while we've validated it is in place for legitimate business purposes, it is missing the necessary restrictions or limitations it should have potentially causing harm. Getting our arms around APIs and where they're being leveraged and used, is a bigger problem than actually securing the APIs themselves."

CONNECTING WITH THE BUSINESS

To achieve a strong connection with the business, Matthew believes in always assessing the risk, coming in with a plan, and ensuring you execute and maintain that plan while remaining aligned to the businesses goals and objectives. He says, "You must have a plan and instill a mindset with your leadership that you are going to do things that are in the best interest of the business and address the areas of the most significant risk first. You must also show leadership exactly why security is important. The plan should include what you've identified as a weakness or risk, how you plan to fix it, and how much money or resources it will require."

Matthew says when coming into a new organization, CISOs need to get in front of each business unit and have productive conversations to understand their line of work, goals, and challenges. He explains, "Sometimes it takes working from the bottom up. Getting ahold of the underlying leadership team in the right way. Not the C-level, but the other people that run the organization and the infrastructure or the application heads and start building processes out that are required."

To effectively communicate with the business, Matthew advises ensuring you have a seat at the table, whether it is with C-levels, other executives, or the board. This could mean scheduling 30-minute meetings to get in front of them and have proactive conversations. Before meetings, Matthew recommends being prepared and tailoring the conversation to your exact audience. He comments, "Understand where your risks are from a business and security perspective. Then take the next step and identify how that impacts your business. Identify what your business is truly trying to protect – is it the brand? Is it the data? Is it the systems? What is it that the business trying to protect? And then pull all that together. Before you even set up a call with the executive team, come up with solutions and say this is where I find the areas of biggest business risk and this is how we are going to address it through avoidance, mitigation acceptance and/or transferal. "

LEADING BY EXAMPLE

"I'm a big fan of team-ship, I need people who are passionate about security, but also I need my team talking, having fun and trusting one another. Most, if not all decisions are made as a team, so that they feel and know their input is valued. I truly feel effective teams disagree with one another from time to time and having a culture that embraces this difference of opinion and encourages respectful debate is extremely important and healthy. That's when great decisions are made. I'm very much against micromanagement and I try to have an open, honest and transparent leadership style. Always being present/available and having regular touchpoints with each team member is critical to make sure they know exactly how well they are performing, so there are no surprises come review time. And if/when they knock it out of the park, I truly enjoy being able to reward them for a job/task well done. A true leader takes pride in the accomplishments and successes of their team members and motivates them to continually better themselves and strive for greatness/perfection, while being empathetic and compassionate during the difficult or trying times."

CYBERSECURITY BUDGETS

Taking a Proactive Approach to Cybersecurity Spending

By Katie Haug

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?

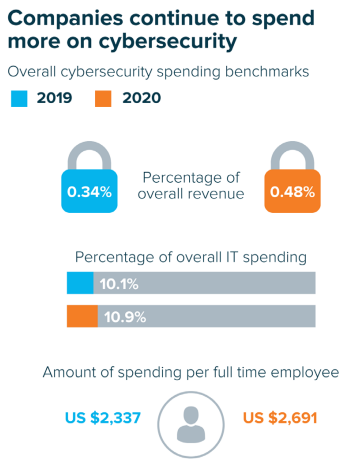
K logix conducted a study with over 200 CISOs across all verticals and the results showed us that 42% said their budget increases 5-10% per year, 48% said it remains around the same and 10% said it is expected to decrease.

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 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

SECURITY BUDGETS

FEATS OF STRENGTH
DECEMBER 2022