FEATS OF STRENGTH

A BUSINESS-FOCUSED INFORMATION SECURITY MAGAZINE

20 SECURITY TRENDS 2020

Cloud
Business Alignment
Automation
A.I. Investments
Zero Trust
Privacy
and much more!

MARCH 2020
KLOGIXSECURITY.COM
617.731.2314

K logix

FEATS OF STRENGTH

2020 CYBERSECURITY TRENDS

MARCH 2020

FROM THE *Editor*

At the beginning of this year we set out to once again interview leading CISOs and security leaders to ask them trending questions in order to correlate the data and share the findings with our information security community. To collect this data, we sat down with CISOs in back-to-back interviews to ask them the same set of questions.

In this issue of the magazine, we share our extensive 2020 Cybersecurity Trends. This article includes the most important trending topics including CISOs' top goals, challenges, areas they are investing in, their approach to consolidation, budget, and much more.

There are two reasons we collect trends on a regular basis. First, the goal of starting our magazine was to provide a platform for CISOs and other security leaders to share their stories. Second, we collect trends to validate and influence our consulting service offerings. This ensures what we offer to our customers is a direction reflection of the challenges and goals of CISOs.

Here are a few highlights from the trends in this issue of the magazine:

- In the 60 pages of transcribed CISO interviews the most commonly used words were: people, cloud, and business.
- Shift Left was mentioned by 54% of the CISOs we spoke with. According to the CISOs we interviewed, Shift Left is the idea of resolving a problem during the first interaction, therefore reducing costs and keeping users satisfied. You can then take those principles and build security around it.
- Security teams are spending almost 50% of their time on the care and feeding of technology versus the security program itself. Many CISOs we spoke with said they hope this number decreases so their teams can think and work more strategically.
- CISOs believe AI is moving beyond a buzzword. Many are actively investing in AI technologies they believe will help their security programs.
- Security budgets have increased for every CISO we spoke with. On average, they increased by 47% in 2019.

I want to thank all of the CISOs and security leaders who contributed to our 2020 Cybersecurity Trends. I hope you enjoy reading this issue of *Feats of Strength*.

Kevin West

CEO, K logix

Magazine Contributors:

Katie Haug

Director of Marketing, K logix

Kevin West

CEO, K logix

Kevin Pouche

COO, K logix

Marcela Lima

Marketing Coordinator, K logix

About K logix:

We provide information security strategic offerings, threat and incident capabilities, education/awareness, and technology services. We craft our services to address specific customer and industry challenges. One of the ways we do this is through our thought leadership, business-focused publication *Feats of Strength*. Through 150+ 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

617.731.2314

2020 CYBERSECURITY TRENDS

THE AVERAGE SECURITY BUDGET INCREASED BY 47% IN 2019

In terms of breakdown, the average security budget is allocated as such:

- 41% on TEAM
- 30% on TECHNOLOGY
- 15% on OUTSOURCING
- 8% on AUDITS/ASSESSMENTS
- 6% on TRAINING

54%

of CISOs said they are focusing on *Shift Left* Security

TOP 2 REASONS WHY CISOs ARE CONSOLIDATING THEIR INVESTMENTS:

1. COST
2. CONVENIENCE OR EFFICIENCY

THE TOP 5 INVESTMENT AREAS FOR CISOs ARE:

1. AUTOMATION
2. CLOUD
3. ARTIFICIAL INTELLIGENCE
4. IDENTITY & ACCESS MANAGEMENT
5. ZERO TRUST

WE ASKED CISOs ABOUT THE TOP CHALLENGES FORCING THEM TO REDIRECT THEIR FOCUS AWAY FROM MORE STRATEGIC TASKS:

- 40% said OPERATIONS
- 40% said LACK OF TALENT
- 20% said LACK OF BUSINESS ALIGNMENT

THE TOP 5 GOALS FOR CISOs THIS YEAR ARE:

1. Focus on Cloud
2. Increasing Security Awareness
3. Leveraging Automation
4. Addressing Privacy Laws & Concerns
5. Implementing Identity & Access Mgmt.

CISOs said their teams spend an average of 43% of their time on the care and feeding of technology

vs. 57% of their time on the security program itself

CISOs believe

20%

of their current technology investments are *ineffective*

ACCORDING TO CISOs, THE TOP TRENDS TO LOOK OUT FOR IN 2020 ARE:

1. Heavier focus on cloud, specifically addressing multi-cloud & hybrid cloud
2. Investments in A.I. technologies
3. Focus on strengthening and/or building a Zero Trust program
4. Privacy laws and regulations becoming more apparent

2020 CYBERSECURITY TRENDS

CONTRIBUTORS INCLUDE:

IAN AMIT,
CSO, Cimpress

MEG ANDERSON,
CISO, Principal Financial Group

JUSTIN BERMAN,
Head of Security, Dropbox

ANDREW BJERKEN,
Global CISO & Privacy Officer, Catalina

DEBBY BRIGGS,
CSO, NETSCOUT

BRIAN CASTAGNA,
CISO, Seven Bridges

TODD FITZGERALD,
CISO COMPASS Cyber-Security Leadership Author

ADAM FLETCHER,
CISO, Blackstone

SUMMER FOWLER,
CIO, Argo.AI

JOHN HEASMAN
CISO, Chegg

DAVID LEVINE,
CSO, Ricoh

RICH LICATO,
CISO, ARC

THOMAS MURPHY,
CISO & Associate VP of IT, University of Miami

KEVIN PAIGE,
CISO, Flexport

CHRIS PORTER,
CISO, Fannie Mae

CORY SCOTT,
Head of Security, Google Nest

SAPNA SINGH,
Cyber Security, Deloitte Middle East

ERKANG ZHENG,
CISO, LifeOmic

The eighteen contributors above represent the CISOs and security leaders who shared their views on the trending cybersecurity topics in this article. Kevin West (CEO, K logix), Kevin Pouche (COO, K logix), and Katie Haug (Director of Marketing, K logix) conducted these interviews to collect the data included in this article. We correlated and analyzed the data in order to provide comprehensive statistics around the hottest trends currently in cybersecurity.

There were many interesting findings, and we are excited to share the content with you in the next few pages. Some of the most prominent topics included thoughtful discussions around the future of the cloud and what it means for security programs, the heavy focus on 'shift left' security, significant research and investment in AI technologies, CISOs focusing on getting back to the basics, and much more.

Budgets were a big topic of conversation and every CISO said their budget had increased in the past year, with valuable dollars spent on hiring/retention, investments in new technologies, and outsourcing. Many CISOs top goals included increasing the security awareness in their organization by spending budget on building a stronger security culture within their organizations.

We also compiled over 60 pages of these transcribed interviews and found the most commonly used were people, cloud, and business.

We want to thank all the CISOs and security leaders who took time to provide thoughtful responses to our trending questions. By taking time out of their busy schedules to influence the trends created by our magazine, they helped us bring meaningful content to our audience.

Please don't hesitate to reach out to us if you would like to be interviewed and featured in our magazine. We also encourage anyone to let us know if you would like to be connected with any of the thought leaders who contributed to this article. We continually encourage our readers to engage with one another to share insight and strengthen our community of cybersecurity professionals.

WHAT ARE YOUR TOP SECURITY PRIORITIES FOR THE COMING YEAR?

AMIT: My main priorities are getting back to basics. I would say my first priority is visibility, being accountable to say this is what we have. And the second one is a derivative of that, which is coverage. Once I have visibility and I can say these are my assets, this is where my data is at, this is how it behaves, and who accesses it, what is the coverage of our existing controls, of the controls that we're deploying? The third one would be better data context. Beyond assets, what really matters? I need to understand who's holding the data and what's more exposed towards the outside, which assets are on a kill chain or susceptible to be attacked. So getting better context as far as knowing what's going on, that's going to enable us to really prioritize more future looking statements like reducing the attack surface. Without having those security basics in place, you cannot assert that statement.

BERMAN: My top priority is always going to be keeping the company safe enough. That means we have the right set of controls to balance the risk reduction we need to make sure there's not a breach with the increasing agility I want to create for the organization, so they're moving fast enough to capture business value. The second priority is looking to how the security team can partner more effectively to not just reduce the risk from a one time or a point in time perspective, but through time. Third is around improving the sources of intelligence that we have in order to make the best decisions possible.

BJERKEN: Privacy enhancement technologies (PET) are one of my key focus areas, as we continue to see shifts in privacy regulations. The Global Security and Privacy (GSAP) group just finished up a two-year transformation phase and a large portion of our security stack was re-engineered. So apart from PET this year, we'll be focusing on processes surrounding the tools we recently implemented, we want to ensure Catalina is getting as much utility from the tools as possible.

CASTAGNA: I have three main goals. First is scaling compliance and security operations. This is a normal part of being in a 270-person venture-backed tech company. And it's figuring out what the right investments are. Second is compliance. Given the nature of our business, which is to enable the analysis of raw next-generation sequencing data at the world's leading academic, biotechnology, government, medical and pharmaceutical entities — which process whole-sequence genomes — we have a lot of compliance requirements. With DNA being some of the world's most personal and private data, we have a very aggressive roadmap that builds upon our existing security and compliance program. Third, I'm hyper focused on engagement with customers and vendors, as security in the cloud is a shared responsibility. From a security perspective, having CISO to CISO conversations with customers, and with our critical vendors, is super important.

HEASMAN: My first priority is driving security earlier into the software development life cycle. We want to ensure developers are not inadvertently introducing security vulnerabilities into our products by catching potential issues as early as possible in the development cycle. Our industry has long recognized that the cost of remediating security issues is high when they are discovered in production. Second is revamping our vendor risk management program and third is improving our logging, monitoring, and alerting within AWS. There's various types of logs that we capture, everything from application logs to host infrastructure logs to AWS logs, but from a security perspective, the challenge is to consolidate these into a unified view and correlate potential suspicious events from each source.

PAIGE: My number one goal is around culture. I'm always trying to embed security into the culture as much as I can by finding innovative ways to provide security awareness training. This may mean hands-on-training, CTFs, or short relevant videos. I find the biggest problems with security training is that it is done as a one time event with possibly boring presentations and/or videos that are not compelling and do not educate. Getting everyone to think about, and understand when there are potential security issues, is job number one. My second goal is around security operations in terms of how we are automating and enabling the business to solve their own problems. I like to use the words "shift left" from an operational perspective. How can I provide self-service and/or automated mechanisms where our employees can help find and/or fix issues themselves with great levels of transparency and understanding of the issues? My third priority for this year is how do we make security easy? How do we find SaaS capabilities that are valuable, and not just a complicated, non-integrated bunch of noise that are focused on solving real problems? For instance, I ask and drive my team how can we fully automate something like incident management the same way our software engineers

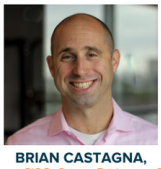

IAN AMIT, CSO, Cimpress


MEG ANDERSON, CISO, Principal Financial Group


JUSTIN BERMAN, Head of Security, Dropbox

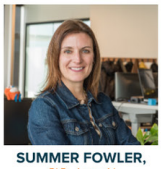

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina


DEBBY BRIGGS, CSO, NETSCOUT


BRIAN CASTAGNA, CISO, Seven Bridges


TODD FITZGERALD, CISO COMPASS Cybersecurity Leadership Author


ADAM FLETCHER, CISO, Blackstone


SUMMER FOWLER, CIO, Argo AI

automate their software pipelines and deployment activities? How can we make security "just work" invisibly and become a thing that blends into the normal day-to-day and not be this thing only a select group of people understand?

PORTER: Digital transformation is one of our top priorities as a company. I have this joke that I tell about digital transformation - there are either companies that are digital native or there are companies that are going through digital transformation, but nobody's actually transformed. We're all caterpillars that are going into a cocoon or are stuck in the cocoon, but nobody's come out as a butterfly...yet. It's a really difficult transformation to make because it's not just a technology transformation. It's a business transformation as well and one where you need to be leaner and more agile, so a lot of the practices that we have codified in IT as well as in security over time, make it really hard to make that transition.

SINGH: From my experience with the oil & gas sector, CISOs top priorities are more inclined towards securing the OT environment due to a significant increase in attacks on industrial control systems in the last couple of years. The convergence of IT/OT has led to significant challenges for CISOs because legacy industrial control systems used for O&G production were not built for cybersecurity. CISOs are challenged by advanced adversaries to protect the industrial control systems from any disruption and to ensure the safety of human lives as cyberattacks continue to lead physical world results. Another aspect is to constantly monitor the organization IT & OT maturity from a security point of view and how new technologies can help to make the cyber infrastructure more resilient to the threats.

WHAT CHALLENGES ARE MOST OFTEN FORCING YOU TO REDIRECT YOUR TIME AND FOCUS AWAY FROM MORE STRATEGIC TASKS?

BJERKEN: The shifts in privacy regulations, specifically CCPA and the impact that it continues to have on ad tech, constantly redirects my team's attention. It requires the team to address controls, develop operational processes, and in many cases re-evaluate vendors, partners, and service providers.

FITZGERALD: In organizations, there's still a lack of business ownership around applications. And I think CISOs are still struggling with that, when you're saying take responsibility for this application, well what does that mean? Well, that means you have to understand who's asking for access to this application and do they need it? It's usually the user manager that does that, but then it requires the business owner to understand how access is provisioned for that application. What levels of access do they have? I think that's a very difficult thing and we really get back to some fundamentals of who really has that access in place.

FOWLER: Tasks that can be automated and orchestrated are BOTH a strategic task and the things that keep my team and I from focusing on other strategic activities. We plan to overcome this by completing projects that will streamline our work – such as building and running a security controls incident response program to address controls that fail.

HEASMAN: With any security program, you're always going to have "keep the lights on" tasks that you can plan as well as unplanned work like incident response that is hard to predict. We're a small team, and incident investigations can cause me to divert people from working on other things.

SCOTT: There are obviously distractions in any given security and privacy program, and it's typically scenarios where you might have incidents that require you to think tactically and address concerns right then and there. I don't think there should be a stigma about, for example, doing incident response incredibly well, because when you come down to trust, trust is consistency over time. And as you build a strong product ecosystem, you have people that get more and more comfortable with your products. But the way that you handle incidents, the way that you handle data breaches, the way that you handle vulnerabilities, will ultimately be a deciding inflection point of whether they continue to trust you. So trust is ephemeral. It takes sometimes years to build, but it can be lost. And so as a result, whilst some people will consider those types of incident response or handling the crisis of the day as a distraction from strategy, it's actually integral to how you build trust.

ZHENG: Since we are a startup, in many cases we wear multiple hats. We have one consolidated security function, which is actually nice, you don't have the situation where the left hand doesn't know what the right hand is doing. But at the same time, we still have to deal with a lot of the noise that comes with security products and operations. Most security organizations, large or

JOHN HEASMAN, CISO, Chegg
DAVID LEVINE, CSO, Ricoh
RICH LICATO, CISO, ARC
THOMAS MURPHY, CISO & Associate VP of IT, University of Miami
KEVIN PAIGE, CISO, Flexport
CHRIS PORTER, CISO, Fannie Mae
CORY SCOTT, Head of Security, Google Nest
SAPNA SINGH, Cyber Security, Deloitte Middle East
ERKANG ZHENG, CISO, LifeOmic

small, have to deal with that noise and we're not different. That is currently the number one distraction or challenge for us overall, especially with limited resources, and I think it will continue to be.

WHAT ARE YOUR CEO'S/ ORGANIZATION'S TOP PRIORITIES FOR SECURITY IN THE COMING YEAR?

BRIGGS: Securing our data, migrating to the cloud in a thoughtful, efficient manner, and keeping the lines of visibility open throughout these processes is of the utmost importance for our organization this year.

FITZGERALD: The CEO's priority this year is really just getting the right CISO in their company, since it's a big problem today. I know there's not as much movement of CISOs in the Fortune 500 these days, which is surprising. I know Forrester did a study in 2017, so things may have shifted a little bit, but I tend to believe things don't shift that fast. They found that the average tenure of a CISO was four and a half years. I always kind of filter out the noise because you see 18 months, 27 months depending on who surveyed who. But what I liked about their surveys, they look at LinkedIn and the Fortune 500, and looked at how long they'd been there. I believe there is an increased recognition of the time it takes to create and execute upon a strategy, as well as the recognition the CISO is needed in the event of a breach.

LEVINE: At the organizational high-level point of view it comes down to protecting our data and our customers' data while supporting and empowering the business.

PAIGE: One of the first things I did when taking the position, is to create a roadmap, and align it to the CEO's objectives and vision. I then made it public and discussed it with all the business leaders and provided public updates for all to see. I think this approach has helped influence the priorities around security. This also starts to drive discussions around budget and staffing as it relates directly to the roadmap. I also think it makes it clear to the CEO that security isn't here to create extra process, or create bureaucracy, but is an important business improvement capability, helping to improve process, and productivity which helps enable the business. I know that as a high growth company, and lots of conversations, one of his top goals is increasing productivity without having to always increase headcount, so I keep that in mind and highlight the areas where security programs can assist.

PORTER: We have a strategy that's set out for the next three years and digital transformation is one of our priorities. Cybersecurity is a huge part of that and we're making sure we're leading our transformation effort. Another priority for the organization is to be a globally recognized, top performing ESG company. That's environmental, social, and governance. Cybersecurity is a key factor in becoming a top performing ESG company because investors and business partners want to be sure a company is appropriately protecting its digital footprint. My job is to make sure that we're in alignment with the senior management and the company in general in what we're trying to accomplish.

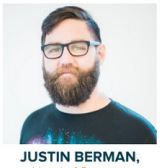
WHAT ARE THE TOP CYBERSECURITY TECHNOLOGY SPACES YOU ARE INVESTING IN THIS YEAR THAT WILL BE TRANSFORMATIVE TO YOUR SECURITY PROGRAM?

AMIT: I'm investing in technologies that focus on where data is and how I map my ability to access and manipulate that data and scale. I want to be able to reduce the set of permissions without affecting productivity and ability to access data. While again, just minimizing that to the degree that if you get attacked or someone's trying to use your accounts, they're not going to have access to the full set. Zero trust is part of it. I'm envisioning when we're looking at technologies that would take that into account, minimize permissions on it, preemptively open it up certain times of year or upon first access by someone from accounting or finances. People do what they need to do and once they're done, their permissions are rescinded. So I want something much more dynamic that's going to be adaptive and true to form.

CASTAGNA: A web application firewall is one, security analytics and security orchestrations is the second, and the third is container security. As part of our due diligence, we are doing pilots and demos with several vendors in order to ensure the best solutions are in place for our customer base.

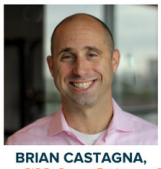

IAN AMIT, CSO, Cimpress


MEG ANDERSON, CISO, Principal Financial Group


JUSTIN BERMAN, Head of Security, Dropbox

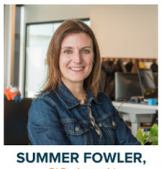

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina


DEBBY BRIGGS, CSO, NETSCOUT


BRIAN CASTAGNA, CISO, Seven Bridges


TODD FITZGERALD, CISO COMPASS Cybersecurity Leadership Author


ADAM FLETCHER, CISO, Blackstone


SUMMER FOWLER, CIO, Argo AI

FOWLER: We are advancing our capabilities in both security and across other teams using our SIEM to monitor and alert on anomalous activity. We also invest heavily in both internal and external penetration testing of our enterprise and products. And going back to some fundamentals, we want to make improvements in our asset inventory and management in order to better address security.

HEASMAN: Automation, automation, automation. Historically when we think about automation in a security team, we first think of incident response because of the emergence of SOAR as a technology to automate response to alerts coming out of a SIEM. But I think there's great opportunity to automate many other parts of information security. We're seeing this in the DevSecOps space with a move towards automated security processes in CI/CD and self-service tooling. Instead of our partners in Engineering and Ops having to come to us to run security analysis tools, these run automatically or on-demand and automatically trigger other processes depending on the results of scans.

MURPHY: CASB, EDR, and next gen endpoint protection. Expanding email security, too.

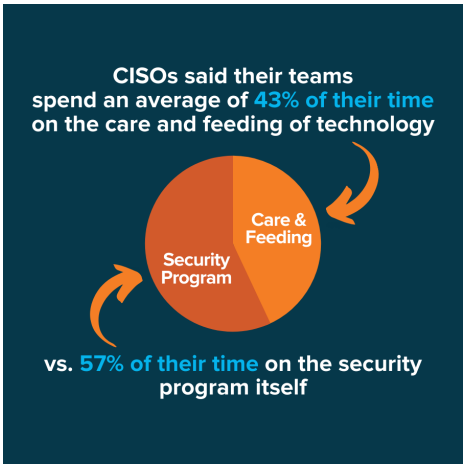
SCOTT: I think we're still going to see a return to a set of fundamentals, making sure that we're actually doing some of the core foundational things right as cloud adoption and SaaS adoption continue. So you have CISOs that are spending lots of time in ensuring they have the right level of visibility into all of their cloud assets, they're collecting the right level of metrics and data in those types of technology, and looking for things that help them enable a more advisory type of role in that regard.

ZHENG: If you look at the way organizations are laying out their infrastructure and operations, we see perimeters are disappearing, so we really need to go back to the basics and understand what we have. The way that works is through a CMDB, a configuration management database to discover, audit and monitor assets. A good CMDB should take into account all of those kind of disjointed point solutions and siloed environments and aggregate them into a holistic view. Additionally, a good CMDB should capture not only the configuration of resources, but also map out the complex relationships among them. This is actually a product we're building internally – a graph CMDB. Other companies, like Lyft, also built asset discovery and management tools on a graph.

HOW MUCH OF YOUR TEAM'S TIME IS FOCUSED ON CARE & FEEDING OF TECHNOLOGIES VS. THE SECURITY PROGRAM ITSELF?

BJERKEN: About 30% of the team's time is spent on care and feeding of technologies. The rest of the time, the team is still very much focused on the program and ensuring we have the right people, processes and technologies, and are addressing risk and safeguarding our clients data. We're in a development stage, so I would expect that after the next 12 months that breakout will shift dramatically to a lot more care and feeding. Then we'll start to look and see where else we have risk that needs to be addressed; it's a continuous improvement cycle.

BRIGGS: As a team, we do our best to balance our distribution of time and resources to these two processes. We have several changes that will be taking place in the coming months, so the focus on the care and feeding of our technologies will certainly increase this calendar year. Since the broader security landscape is always evolving, we are constantly finding new ways to improve and build upon our current security program.



FLETCHER: We probably don't spend as much time on basic care and feeding as we could. We tend to not lock ourselves in a continuous upgrade cycle. We probably don't even monitor enough what the versions of the product are and what features have come out so that we can be on the latest version or the second to latest version. We are more focused on whether the product is doing what we fundamentally bought it to do.

LEVINE: I would say we are spending the majority of our time on supporting the business and operational activity. What we struggle with is finding the time on pure play security initiatives.

PAIGE: Security and technology are very agile by nature, so I think it's important to have an agile and flexible way to deal with work in general. So, I have adopted a two week sprint cycle for our work, and every two weeks does not have to be directly related to the last two weeks. On average we typically spend 25% of our time on care and feeding and the other 75% for program management. Sometimes that's not enough though, and we have to spend 30%, or maybe 40%. But the great thing is that when it goes up to 40%, that probably means there was a major issue to deal with, and If that's the case we are intentional about what we are going to work on. So, we will take work away from our security program for that

JOHN HEASMAN, CISO, Chegg
DAVID LEVINE, CSO, Ricoh
RICH LICATO, CISO, ARC
THOMAS MURPHY, CISO & Associate VP of IT, University of Miami
KEVIN PAIGE, CISO, Flexport
CHRIS PORTER, CISO, Fannie Mae
CORY SCOTT, Head of Security, Google Nest
SAPNA SINGH, Cyber Security, Deloitte Middle East
ERKANG ZHENG, CISO, LifeOmic

particular sprint and push it to the next one. It's all about being intentional and agile. Believe it or not, we'll do a three or four hour session of planning for the next two-week period. I always like being intentional about the work that we're going to do, even about unplanned work.

SINGH: Spending a lot of time on the care and feeding of technology is one of the main problems that we face on a daily basis rather than focusing on the security strategy or program. The adoption of technology tools has increased to combat cyber criminals because the organization's perimeter is no longer limited to on-premise infrastructure and securing infrastructure is no longer possible by firewalls and antiviruses. For example, multiple security endpoint solution agents are deployed to protect systems/servers in an organization. Most time is invested in upgrading signatures, agents, appliances, resolving performance issues, and conflict caused by these tools when they co-exist. We need to correlate events from multiple sources and provide relevant context to analysts to reduce the delay in response and minimize the number of incidents for effective and efficient response.

WHAT PERCENTAGE OF YOUR SECURITY TECHNOLOGY INVESTMENTS DO YOU CONSIDER INEFFECTIVE?

BRIGGS: The processes that we currently have in place are very effective. As an organization, we have always been diligent in tracking the number of tools and technology we are utilizing to ensure we are not over-purchasing or inappropriately allocating resources.

FITZGERALD: I'd say probably 30% to 40%. I think historically people get a tool, they bring it in and run the tool for a while, but people change roles. There's really not the training budgets associated with bringing the tools in or the retraining of the people. There's also not the figuring out how to really use the tool or the money to integrate that tool with the other tools that you just bought. That's usually not in the ongoing budget.

HEASMAN: I wouldn't say any of the technologies we have are ineffective, but I would say that we are working on tuning some of them to make them more effective. Technologies that produce a large number of findings require tuning to minimize false positives and ensure high impact, and high confidence findings are correctly flagged as such. It's common to hear of incident response folks talking about alert fatigue, with overworked analysts trying to keep up with the endless streams of findings that many tools crank out.

PORTER: I would say that for most companies there's probably a good 20% of technologies that are either ineffective or will soon be replaced. There's some rationalization that is going to take place where there are a lot of different overlapping features, functions, and capabilities. Companies need to prioritize the most important features and technologies that they have and be thoughtful in how they cut some of the others. We should be constantly looking at our technology stack, and constantly looking out into industry and the startup community to see what technologies are coming around that can supplant what we currently have or give us a new capability that we don't currently have. Help us fight the bad guys.

IN THE PAST YEAR HAS YOUR BUDGET INCREASED OR DECREASED?

AMIT: I would say our budget increased between 15% to 18% overall and in terms of split between investment, it's about 40% headcount, and the majority of the investment is towards technology, being able to cover more assets for our businesses, provide more services and products. We're now operating as an eternal MSSP to our customers. Due to that model, the more adoption that our businesses and our customers have, the more we need to have a bigger budget to support that. I think it's a nice healthy growth that's mostly driven by demand from the businesses rather than by our internal security demands.

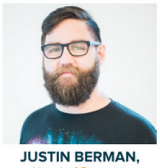
LEVINE: The security budget has either remained neutral or increased some over the past few years. Our scope has also expanded as well and would need to be factored in. As far as the mix goes, today we are 50% salary related, 12% outsourcing and 38% technology.

MURPHY: More of existing IT budget is being directed to security. Because of talent shortages, we want to increase our staff development, training, and certifications in each year's budgets to make sure we attract and retain the right people. In terms of the technology, I expect spending would probably level off at some point after key investments and system upgrades are complete.

PORTER: We find ourselves continually re-evaluating our budget to make sure we are able to put the proper controls in place to mitigate risk and protect our infrastructure. Think about what has happened over the last 10 years. As things start moving outside of

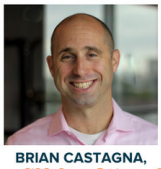

IAN AMIT, CSO, Cimpress


MEG ANDERSON, CISO, Principal Financial Group


JUSTIN BERMAN, Head of Security, Dropbox

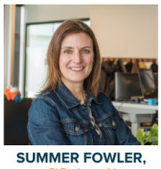

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina


DEBBY BRIGGS, CSO, NETSCOUT


BRIAN CASTAGNA, CISO, Seven Bridges


TODD FITZGERALD, CISO COMPASS Cybersecurity Leadership Author


ADAM FLETCHER, CISO, Blackstone


SUMMER FOWLER, CIO, Argo AI

THE AVERAGE SECURITY BUDGET INCREASED BY 47% IN 2019

In terms of breakdown, the average security budget is allocated as such:

- 41% on TEAM
- 30% on TECHNOLOGY
- 15% on OUTSOURCING
- 8% on AUDITS/ASSESSMENTS
- 6% on TRAINING

your data center, you're now operating in multiple data centers with multiple cloud partners in multiple regions. The surface area of what has to be controlled and protected is expanding at a pretty rapid velocity, while at the same time the bad guys are also accelerating. Ultimately, it's a race to make sure that we're protecting the surface area as fast as it's expanding and doing it with solid governance practices. I think that's one of the reasons that security budgets overall are increasing as much as they are. But it can't last forever, and I expect that there will be a tail off to budgets at some point.

ZHENG: Our budget has certainly increased. For us, it more than doubled this year. We are in a bit of a unique situation though, because we are an early stage company growing rapidly, both from a company size and operations standpoint. Security needs to be somewhat proportional to that growth. Second, we are kicking off a new initiative around FedRAMP, so the increased budget reflects the need and the cost associated with getting that certification. In future years, I think it would stabilize with some increase, but most likely not doubling again.

IF YOU RECEIVED THE GREENLIGHT ON ANYTHING YOU ASKED FOR, WHAT WOULD YOU DO THAT YOU'RE NOT ABLE TO DO RIGHT NOW?

AMIT: Last time I had a conversation with the CEO, he actually asked me for some more activities. I truly don't have anything right now that I'm being held back from doing. I think that that's one of the major things I like about what I do is we have a very open, honest conversation between the executives. I don't think there's anything that I managed to articulate in terms of risk versus reward, how we're managing things and providing full-on executive context that was not green lighted. So honestly, better pay for my team, more time off, more training, more education.

BERMAN: One of my personal passions is around the data-driven approach to security, and part of that is the intelligence piece. The part I would accelerate is controls assurance. I believe it is time we drive consistent engineering-like testing methodologies into security. When you deploy a control, you should not just be able to track whether that control is on or off, but how well it's stopping what you think it needs to stop. So implementing that holistic testing across the entire organization would be a thing I would increase funding on if I could get the greenlight for anything.

FITZGERALD: I think CISOs should be asking for money for AI, orchestration, and automation. The number of people with these skills are limited and many organizations do not have them on staff. There are some companies that have gone down the path of orchestrating, it's not necessarily artificial intelligence in that sense. It's looking at every manual process that somebody is doing and automating that. That frees up the security people so they can look at high value opportunities, which should always be the goal.

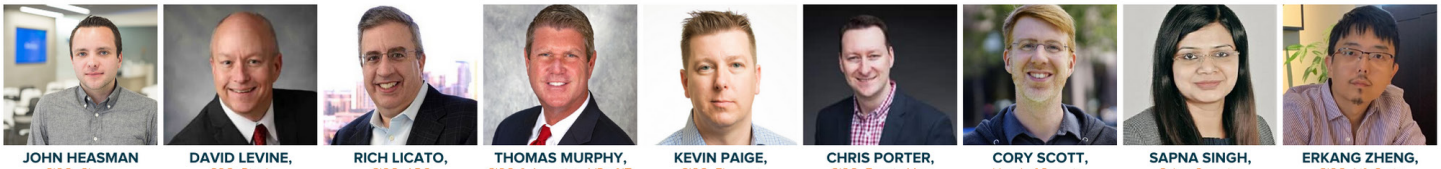
FLETCHER: It would be an increased amount of data classification. I don't know how it would get implemented without too much friction, but I would want to more granularly understand the different layers of confidential, and when certain data should be limited to a very small group of people. With that detail, I could implement more controls and sleep a little bit better knowing that certain things were more protected than others and that some of the worst scenarios I could imagine would be very unlikely to happen. A close second would be perfect automation around access and entitlements to all systems throughout the employee lifecycle.

IF CISOs WERE GIVEN THE GREENLIGHT ON ANYTHING THEY ASKED FOR:

- 63% would ask for more budget to hire/retain staff
- 18% would ask for more budget for technology investments
- 18% would ask for more alignment with executives

FOWLER: I am fortunate that I face far fewer internal challenges in a company that prioritizes safety and security above all else. If I could do anything, I would attract and retain some more top talent – and quickly!

MURPHY: I would take bigger steps toward perimeter-less security. Next generation firewall services that would help us with visibility would be great. When you look at the cost of a complete



JOHN HEASMAN, CISO, Chegg | DAVID LEVINE, CSO, Ricoh | RICH LICATO, CISO, ARC | THOMAS MURPHY, CISO & Associate VP of IT, University of Miami | KEVIN PAIGE, CISO, Flexport | CHRIS PORTER, CISO, Fannie Mae | CORY SCOTT, Head of Security, Google Nest | SAPNA SINGH, Cyber Security, Deloitte Middle East | ERKANG ZHENG, CISO, LifeOmic

core network and firewall re-architecture, that cost either competes with other budget requests or consumes an entire budget. Turning the aircraft carrier a little bit on that just takes time.

SCOTT: At Google, I'm kind of like a kid in a candy store, I'm in a scenario where I'm working with the best technologists in the world. It's an incredibly hopeful and collaborative culture. There's really not much that I wish for. Of course all of us want more resources, more headcount, all of us want dedicated recruiting 100% of the time to finding the best talent and bringing them in for you and all those other things. At least from my experience to date, anything that I felt would be best to protect our users and to respect their privacy, has been provided. So I'm kind of lucky. So it would be more people, and then sort of figuring out how can we improve our processes right now? And yes, there would be some additional vendor spend, but again it's not like I feel our program is missing some sort of major component.

WHAT ARE THE DRIVERS FOR CONSOLIDATION WITHIN YOUR PROGRAM?

AMIT: For me, the typical drivers of consolidation would be optimizing our operations. Meaning automating things and freeing up my investment in human resources to do other things that are not just product maintenance. I want to make sure that my team is challenged in the long run. They need to have a good career path that's challenging to them and that they are learning new skills. If I can find ways to optimize that by consolidating and optimizing certain processes or existing products, we will absolutely make an investment there. It might even be counterintuitive from a financial perspective initially but if I can see a long-term return as far as investing in human capital, I would absolutely buy it.

BERMAN: I think the nice thing about having a solid security engineering team inside Dropbox is that when we identify a problem to solve or a set of jobs to be done by the security team, we're always considering what we already have and if it solves a problem. I think of consolidation as being a part of the same processes you would run normally around figuring out how to solve a particular problem, and doing so with an eye towards the total cost of ownership or the total reward for the investment as opposed to it being a thing where in isolation you want the perfect solution to one problem.

CASTAGNA: As a growth stage company, it's a little bit less about consolidating and more about taking the initial investments that we've made and refining them. In addition, we are making very strategic decisions on what we invest in and why. Because we're early stage, high growth tech, things are changing very, very rapidly. It's important that we're thinking about our security investments, and we also need to be able to pivot quickly. So as we're refining that approach, it's got to be done in a very fluid manner, and it's also got to be done looking at where we expect to be in two years.

FLETCHER: Most of the things that we use, outside of the fundamentals, are features and should probably be wrapped into a broader platform product. There are two schools of thought here: one would be, there's consolidation that's really good and really creative, and if you get a platform that pulls together multiple best in class products seamlessly, then it can be highly effective. The other school of thought would be, if there's one vendor out there that is really good at one thing and good enough at five other things, then maybe it just makes sense to switch and reduce that complexity.

HEASMAN: Our main goal of consolidation is to simplify our program to allow us to be as effective as possible. Business is complex, security is complex, and our program is complex. Consolidation means I have one less vendor to deal with, one less technology to manage and that matters because approximately 25% of my team's time is spent on the care and feeding of these technologies.

MURPHY: The drivers for consolidation are mostly split between cost and convenience. As is the case in many higher-ed institutions, funding is distributed through budgets to schools and departments. If they want autonomy and they can afford it, they get it. But on the other hand if centralizing services, like identity and access, email or cloud services, gives us better economies of scale, consolidation just makes more sense.

PORTER: Cost is always a consolidator, but it's not just for reducing your operating costs or operating budget for what you have, but also reallocating funds. Some of it might involve having to shift my investment somewhere else because I need to create

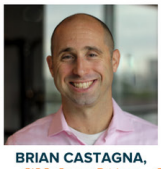

IAN AMIT, CSO, Cimpress


MEG ANDERSON, CISO, Principal Financial Group


JUSTIN BERMAN, Head of Security, Dropbox

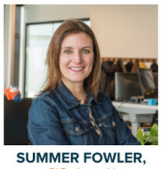

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina


DEBBY BRIGGS, CSO, NETSCOUT


BRIAN CASTAGNA, CISO, Seven Bridges


TODD FITZGERALD, CISO COMPASS Cybersecurity Leadership Author


ADAM FLETCHER, CISO, Blackstone


SUMMER FOWLER, CIO, Argo AI

a new capability. Another is around risk and controls, what are our highest risks that we're trying to protect the company from? What are the controls that we're putting in place to help mitigate that risk? And then by making changes, how are we affecting the residual risk in our organization? It's a combination of capability development, doing the consolidation on a risk-based basis, making sure you're still covering all the controls across the organization that you need to control, and then putting all that information together as a part of it.

WHAT ARE THE TOP INDUSTRY TRENDS YOU EXPECT TO BE MOST PROMINENT IN 2020 AND BEYOND?

BJERKEN: AI enabled security is a big trend as security practitioners are looking to close the gap; improved analytics offers some great options. We want to increase our situational awareness and ultimately reduce the time it takes for us to actually mitigate an attack. On that same token though, as we add more AI and improved analytics, I believe privacy concerns are going to be competing interests. Security wants to collect more data and do advanced analytics to build actionable baseline profile on individuals while privacy pushes to give more control over personal information into the hands of the subjects. It will be interesting to see how this flushes out over time.

BRIGGS: First is viability both on-premise and in the cloud from a single console. Unfortunately, there are not enough cloud security experts, which reinforces the necessity to leverage the tools and technologies that have been successful with on-premise operations and utilize them in a multi-cloud environment. Second is streamlining and improving the tools we use. Not only do we need to be more diligent about the streamlining process, but we need to continue incorporating more intelligence into these systems. Third, increased demand for talent. We are all going to have to get more creative in terms of where we find security team members. I have personally found that having interns on my staff allows me to teach meaningful job skills while helping the broader team to see if the candidate has the aptitude that we need.

FLETCHER: I think we will continue to see migration to the cloud with Platform as a Service, Software as a Service, and Infrastructure as a Service. I think that the largest companies will probably be hybrid for a very long time. I think companies that have 25-to-50,000 endpoints and below are probably moving to the cloud, moving to Infrastructure as a Service platform, and are out of data centers within three to five years. Newer companies, if they haven't already moved completely into the cloud, that's happening fast. I think you'll see a continued adoption of these PaaS and SaaS providers, which will then create opportunities for security companies to help manage that, both on the strict security side of identity and access management, of configuration, of monitoring and alerting and response and things like that, as well as the ops side of things.

FOWLER: Organizations will continue to make adjustments to their cloud strategies and execution. We will also see advancements in 5G present new IoT opportunities and challenges. Automation and orchestration will also continue – and sometimes be blanketed under AI or machine learning (at times incorrectly).

LEVINE: First, cloud will continue to be a big push. Second, all things Privacy related. Third, security continuing will be a more strategic business partner

MURPHY: Security in hybrid and multi-cloud environments is going to be right at the top of trends. This being an election year I expect there will be an increase in phishing as people want to stay current with candidates and sign up for mailing lists. Also, low friction endpoint solutions that work with BYOD to extend posture.

WOMEN IN CYBERSECURITY

Sapna Singh, Cybersecurity, Deloitte Middle East, shares her work influencing women in Cybersecurity:

SINGH: I am working with various communities to support women in Cybersecurity. I am an active member of the "Women in Cybersecurity Middle East" Group and co-organizer of the Kuwait affiliate of Women in Cybersecurity Middle East. I coordinate with cofounders and organize Cybersecurity influencer talks, knowledge sharing talks and technical talk for our women members across the region.

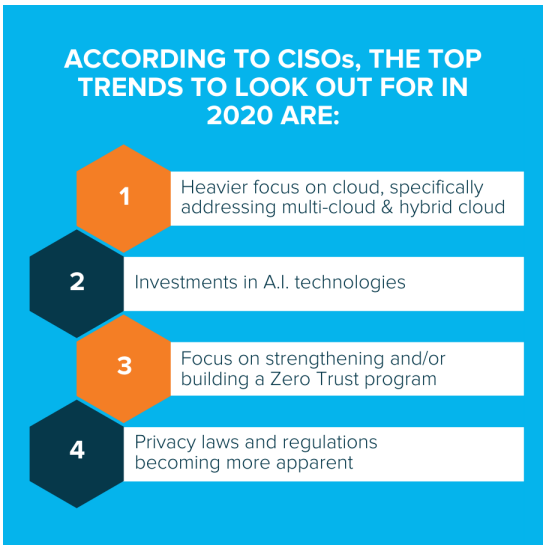
I am also in the core team of Women in Cybersecurity (W-CS), a special interest by Information System Security Association (ISSA) to support women in Cyber in India. As a group, we also organize physical meetups and workshops to support, empower and guide women in Cyber.

I lead the "Deloitte Women in Cyber" group for the Middle East where our objective is to hire, support & retain more women in Cyber. While working with these communities my main goal is to:

- Educate and train college students for Cybersecurity and to provide Cybersecurity career advice.
- Support women who are interested in joining Cybersecurity and guide them on how they can join the domain.
- Retain women who are already in Cybersecurity and provide mentorship for their success.

JOHN HEASMAN, CISO, Chegg | DAVID LEVINE, CSO, Ricoh | RICH LICATO, CISO, ARC | THOMAS MURPHY, CISO & Associate VP of IT, University of Miami | KEVIN PAIGE, CISO, Flexport | CHRIS PORTER, CISO, Fannie Mae | CORY SCOTT, Head of Security, Google Nest | SAPNA SINGH, Cyber Security, Deloitte Middle East | ERKANG ZHENG, CISO, LifeOmic

PAIGE: With more and more privacy regulations being released which are holding companies accountable for proper usage, storage and movement of personal and customer data, I think "privacy engineering" is going to become a real thing. I think it's going to be forced out of a legal and compliance issue, and into a real engineering issue to solve holistically, as part of all engineering implementations specific to how software products are collecting and dealing with data in general. The other major trend I think we will see is related to my thinking that CASBs are kind of dead, they became too much of a complicated point solution. So, I think we are going to see more solutions related to helping manage and govern cloud SaaS solutions that are highly opinionated and integrated into common toolsets.



SINGH: The human element in cybersecurity is a big trend this year. Many organizations have been focusing on technologies and forgotten about the human element. Security Analysts work 24/7 to resolve critical incidents, something that can lead to mental health issues, that are more often overlooked. CISOs are also under constant stress to secure organizations infrastructures against cyber-attacks, and pressured to deal with ever-growing threats. Cybersecurity teams are expected to secure thousands of employees, critical infrastructure, and confidential data. We need to find creative ways to engage users and help them understand that cybersecurity is everyone's job.

SCOTT: I think you're going to continue to see an evaluation of what types of security program activities are actually best risk-aligned. For example, traditional security awareness and training and the requirement of the users to participate in certain types of security actions, as opposed to more secure by default types of frameworks. I think you're in a contingency of reevaluation of those types of things, and you have scenarios where you can set up good boundaries for how engineers or developers can deploy services or deploy technology to end-users where it's essentially tied to already existing, well established security patterns. I think you're going to continue to see people wanting to do that rather than bespoke security, adding little bits of security in everything that they do.

ZHENG: We have seen two great trends in cloud security – namely infrastructure as a code and "shift left". A promising new trend I see is security teams becoming engineering teams. It's not a product trend, but a trend around the organization culture and skills of security teams. We still see a tremendous shortage in security skills and talent, part of that is because the new way security needs to operate is more like engineering teams, in order to keep up with the speed of DevOps and to stay relevant. In many of the organizations we work with, we see that. On our product side, we work with many large cloud native companies, and they have all adopted engineering operating models for their security.

DO YOU CONSIDER YOUR SECURITY PROGRAM TO BE COMPLEX?

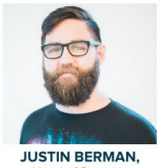
BERMAN: At an abstract level, anyone who says security isn't complex doesn't really understand security itself. I think my job, and the security team's job, is to abstract the complexity away from the rest of the company. It's important for us to build technology and processes and even training and capabilities that make it easier for the company to move forward rapidly, and in fact removes security from the set of considerations they have to focus on in as many places. I'm not saying no one should care about security, but I am saying people should care about the nuanced and small part of security which is really relevant for their specific job function as opposed to a different mindset that I've heard, which is everyone is on the security team, something I disagree with.

CASTAGNA: Yes. I think most security programs are complex, but our complexity is driven by the nature of our business within genomics — which is highly complex in itself, the nature of our customer base — which is enterprise and government and the nature of operating in cloud and shared responsibility model and the technology stacks. I think the complexity of the security program is often inherently based on the level of security that's required for the business. The more you get into data types or businesses that have sensitive data, I think there is inherently more complexity associated with that, more investment that's required and earlier investment that's required.

HEASMAN: Yes, I think all security programs are complex since our goal is to manage risk to the business and businesses are

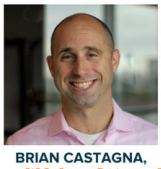

IAN AMIT, CSO, Cimpress


MEG ANDERSON, CISO, Principal Financial Group


JUSTIN BERMAN, Head of Security, Dropbox

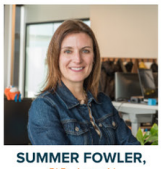

ANDREW BJERKEN, Global CISO and Privacy Officer, Catalina


DEBBY BRIGGS, CSO, NETSCOUT


BRIAN CASTAGNA, CISO, Seven Bridges


TODD FITZGERALD, CISO COMPASS Cybersecurity Leadership Author


ADAM FLETCHER, CISO, Blackstone


SUMMER FOWLER, CIO, Argo AI

inherently complex. In Chegg's case we've largely grown through acquisition, and integrating acquired companies is always a complex process. As a business evolves over time and shifts direction or priorities, this leads to deprecated products, services and technology stacks that are still operational since they generate some revenue but may only be nominally supported as they are not the core focus of the company. These shifts contribute to the layers of complexity for any security program, though dedicated initiatives around technical debt reduction can help manage these down.

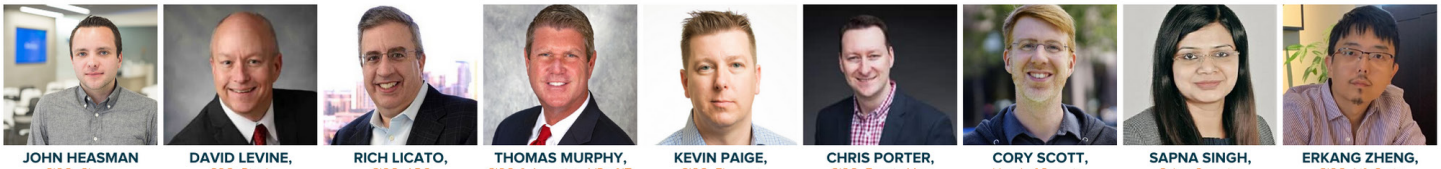
MURPHY: Yes, it's complex because the mission of the University of Miami focuses on four areas: education, research, innovation, and service. We have eleven schools, including a medical school, a hospital and clinics throughout South Florida. The complexities lie in weaving a security program that works for all areas of the University while supporting our mission.

WHAT DOES "SHIFT LEFT" MEAN TO YOU?

BERMAN: When people talk about shifting left, what they often mean is security getting involved earlier and earlier in the cycle of technology development. They should be involved in ideation, design, or the initial product work as opposed to only being involved after or during the implementation of that technology. I actually think "shift left" is much more about how you can make your investment earlier in the technology life cycle so you spend less time, energy and money for the entire organization on dealing with security problems. So to me, shift left is much more about how you can help the organization spend fewer resources and get more total security as a result.

PORTER: We've been using the term "shift left" for at least five years. During that time we started shifting left in our application development where we moved a lot of our security testing into the developer's tool sets. The transition led to developers testing their own code when they're writing it, allowing for quick fixing at the beginning rather than waiting until after it goes into production. That has had a pretty dramatic effect on the quality of our code that's coming through and the number of security related defects that are making it through the process. The concept has been around for a long time. I think it's really gained a lot of traction in recent years, but a lot of people think about shifting left in terms of code development. Ultimately you want to "shift left" all the way into business initiatives. Like when you're doing cost benefit analysis, looking at business value created, technology risk, operational risk, cyber risk, resiliency risk, all need to be looked at upfront. And if you look at all that stuff up front, it'll take care of itself a lot better as it follows through to when it actually gets to the value creation aspect.

SCOTT: "Shift left" came from an IT principal. Essentially, if you imagine a very traditional IT help desk 10 years ago, and you called the IT help desk and said your email was not working. They then route it to the email team. And I'm going to file a ticket and shift it over to the email team, and then they'll look at it, fix it, and route it back. In this example, the idea of shifting left is instead of making the mail admin do it, they shifted it left to the help desk and gave the tooling to the help desk so they can fix it themselves. Most corporate enterprises have become much better because of that "shift left" strategy. The idea is that if you can get the first interaction to resolve the problem, you've reduced costs and the users are happier. You can then take those principles and you build it around security.



JOHN HEASMAN, CISO, Chegg
DAVID LEVINE, CSO, Ricoh
RICH LICATO, CISO, ARC
THOMAS MURPHY, CISO & Associate VP of IT, University of Miami
KEVIN PAIGE, CISO, Flexport
CHRIS PORTER, CISO, Fannie Mae
CORY SCOTT, Head of Security, Google Nest
SAPNA SINGH, Cyber Security, Deloitte Middle East
ERKANG ZHENG, CISO, LifeOmic

MICHAEL CHARLAND

GLOBL ISO, HARTFORD STEAM BOILER, A SUBSIDIARY OF MUNICH RE

HEADQUARTERS: Hartford, CT (Hartford Steam Boiler) and Munich, Germany (Munich Re)

EMPLOYEES: 41,400+ (Munich Re)

REVENUE: $52 billion (Munich Re)

After spending 21 years working in emergency services, Michael Charland moved into a number of IT roles, eventually leading him to a more security-focused career track. As Charland worked in security roles with increasing levels of technicality and responsibility, he transitioned into managerial positions where he had an opportunity to leverage his communication and business skills. As he matured in his career, Charland had exposure working with other C-level executives to help drive security maturity and grow programs to meet the demanding needs of the business.

Currently the Global Information Security Officer at Hartford Steam Boiler, a Munich Re subsidiary, Charland has responsibility for a global organization inside of a larger global organization. He says, “My organization has seven subsidiaries and two additional business units acting as self-standing business organizations. I currently lead information security in the verticals of finance, hospitality, IoT, insurance/reinsurance, cybersecurity, energy, inspection and engineering of building and other services. I’ve also led information security in the healthcare and banking verticals in the past.”

Charland was attracted to his current role at Munich Re/ Hartford Steam Boiler not only due to the global nature, but because of the numerous subsidiaries in a variety of verticals and the emphasis the organization put on the importance of information security. Reporting into the Global CISO, Charland says it was evident security had a clear vision of direction and defined path for growth.

STRATEGIC SECURITY GOALS

For the year ahead, Charland is focusing on three main goals: increasing security awareness, gaining buy-in and participation from IT and the business, and continuing to grow the program by providing strong information security.

Charland explains, “The basic root of my goals this year is to increase security awareness and bring the organization fully online with the understanding that it takes each and every one of us to protect the organization and its assets. We need to get back to basics as well. I understand that we all enjoy the new flashy devices and “Next Gen” toolsets, but if we don’t manage our assets or properly patch, the fancy tools will not increase our security posture. Information security can be a difficult topic for people because your individual goals are constantly changing with the landscape. Security changes moment by moment, new vulnerabilities are found each day, ways to bypass antivirus and other security tools are developed or released into the wild daily, if not more often. It reminds me of being in law enforcement. We work continuously to learn new skills then train to develop and deploy these skills, but often, our methods

become outdated almost as quickly as we deploy them."

THE PEOPLE FACTOR CHALLENGES

In order to accomplish these goals, Charland believes the top challenge he must overcome is the people factor. He believes it is vital to get buy-in from everyone within the organization, so they understand the key role they play in protecting the brand.

He comments, "We need to get the buy-in from people, because I can put tools in all day long. We could do logging and put things in place to help protect us, but if one person clicks on a phishing attempt, then we're chasing the path of being under attack. If one person goes to a website and puts information in that they shouldn't, there are so many avenues that are open to the person being socially engineered."

COMMUNICATION AS THE KEY TO SUCCESS

Charland believes communication is critical to his success. In his current role, not only does he communicate with peers in the senior leadership area, but he also communicates regularly with line-staff to understand where they are facing challenges. He says the more everyone speaks with each other, the more open they are inside the organization, and in turn, the more successful they will be.

Building relationships and communicating with other C-level security leaders is also crucial to Charland. He explains, "Communication is one of the ways criminals have always stayed ahead of us. In law enforcement, criminals do not have to follow work hours or rules, and they will use anyone and anything they can to achieve their goal. On the other hand, we must work within rules, laws, and parameters. Our hands are tied because the privacy laws of some countries do not allow tracing of certain end user activities. To combat the fact that we have limitations, we all need to communicate regularly. Build up your CISO and information security network and be there for others when they call you at 10pm on your vacation saying they need a helping hand. We all need to help each other, discuss our pain points, and share solutions we are using to resolve them freely inside our community. That is the only way we stand a chance to keep up. I have had the opportunity to make connections and build relationships with some amazing and incredibly talented individuals in our field. All it took was reaching out, being myself, and being willing to help them in any way. Take the time to build your network. Trust me, it is great to have a network to reach out to and assist in problem resolution."

BUDGET BUY-IN AND APPROACH

Before budget allocations, Charland works to determine where to make investments that will make the greatest impact for the security program. This comes following partnership with IT and the business to determine how the business and IT landscape may change in the coming year.

Charland approaches budget discussions in a strategic manner, especially due to the global reach of the organization. He says, "First I have to have local buy-in. In our case, the local is actually global. It's local to me, but global for all of our organizations. And then budget even rolls up from there to the mother company, who also must have buy-in to the budget. So it not only happens here, but then goes up an additional level to the global level (CIO, CEO, and CISO). It's an interesting situation because we're a global company inside of a global company. You don't see that very often."

He balances current needs with the needs of the year ahead and understands that an over-reliance on tools may not be the right answer. He explains, "You can't just drop a tool in to solve a problem. A new tool requires resources to run it and evaluate the output. Also, that resource needs a backup. It is a balance based on the current needs and those of the upcoming year. In 2008 the IT industry began laying people off and not replacing them, but instead having individuals do more in their roles. This trend has continued. So, I do my best to run with lean teams utilizing highly effective individuals who openly communicate within their team and outside."

MANAGING SECURITY FOR THE CLOUD

"Although many organizations have already begun moving to the cloud, they often have not taken time to provide training to their IT and/or security teams on the differences of how to manage security for cloud. There are many changes in how we manage security in the cloud based on whether the solution is SaaS, IaaS, or PaaS. When moving to cloud, we need to make sure that compliance is in place for our cloud configurations. Automation must be used as much as possible and we must regularly confirm that a person has not accidentally opened a hole causing a security vulnerability. Several times we have seen a person accidentally cause an opening that results in a breach. We need to understand and automate processes with policy and automation in place prior to moving to new technologies."

DMITRIY SOKOLOVSKIY

CISO, AVID

HEADQUARTERS: Burlington, MA

EMPLOYEES: 1,400+

REVENUE: $413 Million

For the first 10 years of Dmitriy Sokolovskiy's career he had first-hand experience with servers and datacenters, NOCs and SOCs, and consulted for defense contractors, public and private financial and medical companies, and non-profits.

Sokolovskiy then spent eleven years working at a security vendor, where he first built and managed the implementation arm of the professional services organization for Americas, personally participating in incident response and remediation for some of the largest breaches in US history. Later, he served as a Cloud Security Architect, helping protect the organization's SaaS products utilizing CSA CCM and CIS CSC.

Currently, he is the CISO at Avid, a technology and multimedia company headquartered in Burlington, Massachusetts. Making the transition to Avid meant leaving an organization servicing a specific niche of the information security marketspace and moving to a holistic CISO role at a forward-thinking technology company. As CISO, he leads the build-out of the information security and privacy program, covering corporate and customer-facing cloud environments, and hardware and software products.

He explains, "The move to Avid was something I wanted to do, and I felt like I had a lot of experience both running a team in information security but also having seen all kinds of deployments and all kinds of issues over the years. I could combine those experiences together and apply it as a broad-spectrum application of security."

BUILDING A PROGRAM FROM THE GROUND UP

When joining Avid, Sokolovskiy understood he was faced with a challenge as their first ever CISO, but it was a journey he was excited to embark on. The organization had no dedicated security function and Sokolovskiy was able to come in and implement a security program on his own terms as opposed to coming in and taking over an already established program.

This green field opportunity for Sokolovskiy was fully supported by senior leadership. To take on the somewhat overwhelming task of establishing a strategic, strong, and business-aligned security program, Sokolovskiy approached it by focusing on prioritizing and controlling his time.

He explains, "It's important to control your resources. That will set you up for being able to do whatever you want to accomplish, if you do it correctly. It will also make sure you clear up any expectations that executive management might have about what you can accomplish. Everyone is on the same page that we're not trying to build Rome in two days. I could work 120 hours a week and not cover all of the things that are coming in within that week. It's important to be able to prioritize and to control your time really well and apply it to the most important things. I focused on continuously reviewing,

prioritizing, reprioritizing, then working without interruptions. As the team grew I made sure that they did the same, utilizing available resource management tools as needed. I've focused on managing resources well, concentrating on the important things, being clear about what we can't do, and continuing to provide good advice."

ASSESSING, STABILIZING, AND FORMALIZING THE SECURITY PROGRAM

It was vital for Sokolovskiy to make sure unplanned work, emergencies, and incidents did not derail his strategic plans and focus. Instead of reviewing and assessing the organization against a specific framework right at the beginning, he instead assessed against a live snapshot of issues they were actively facing, then worked on applying controls, process, redesign, or tools if necessary. Now a year and a half in, he says they are in a position where they can take a framework and apply and measure against it in a structured way without being continuously interrupted by incidents or attacks.

He says, "We chose the NIST CSF framework because it was distilled from several more expansive frameworks, yet made it much easier to follow and measure ourselves by. We're finalizing the formal self-assessment and gap analysis and we'll work on the structure remediation plan. But I can't stress this enough - that even before that's done, we had to "stabilize the patient", and only then use a more formal, structured approach to long term remediation."

FOCUSING ON SECURITY AWARENESS AND RISK DECISIONS

One of the top goals Sokolovskiy is currently focused on is information security awareness. He says his approach involves multiple angles including computer-based training similar to an online university for standardized mandatory training, as well as dedicated lunch and learn type activities and ad hoc agenda-less Q&A meetings.

He comments, "We are scheduling dedicated lunch and learns that are structured, goal-based lectures for employees, but we don't make them mandatory. Combined with that, we also have ad hoc agenda-less, but still structured, meetings. 'Lean coffee' is a style of meeting where employees come in and bring their topics and then everyone votes from the topics that were submitted. And we talk about them in order of voting. And sometimes we don't cover everything. We may leave some topics until the next time, but it's this continuous live information security Q&A that we make available to everyone in the company. Employees are getting access to trained information security personnel with experience, and we are getting continuous publicity with the employees to make sure they remember that information security exists. It's this continuously available source of information about security that becomes useful in their personal lives, which inevitably makes them more secure in their professional lives as well."

Another one of his top goals is changing the thinking around risk decisions. Their approach is not to have the information security team own risk decisions, but to be a guide to the business when they are making such decisions. Instead of the business coming to Sokolovskiy and asking if he approves a specific project, he is trying to institute a shift where business comes to information security to work together to identify risks and the risk level. Risks of different levels are then presented to management for written approval within the business unit, depending on the level of risk.

He explains, "Instead of being the blocker, we are a partner, and we are helping the business identify the risks on their level and then work with them to see if there's a mitigation control. But at the end, the decision and responsibility for that risk stays within the business. When it's owned by them, it becomes a very different process. Introducing this flow and changing the way business approaches risk decisions is probably the second biggest priority for this year."

RISK AWARENESS AND DECISION MAKING

"Information security is never going to be about technical solutions. All the technology out there, it's only a solution to one problem or several problems, but ultimately, it's not going to achieve "security". It must come as part of this standardized and holistic decision-making approach. It has to be based on user and business awareness of the fact that every decision will have risks, and that the information security team is there to help them identify and measure those risks, and help figure out how to mitigate those risks in the most effective and cost effective way possible. And when they have that thinking and when reaching out to the security team for quick verification becomes second nature, then we can say that we've made the company secure. Every company's going to get breached. It's this risk awareness-based decision making process that's going to allow you to survive with minimal impact, and keep the company, the employees and the customer information secure."

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446