FEATS OF STRENGTH

A Business-Focused Cybersecurity Magazine

REGULATIONS & COMPLIANCE

ORIENTING YOURSELF IN THIS EVOLVING LANDSCAPE

IN THIS ISSUE:

SCOTT KING
CISO, ENCORE CAPITAL GROUP

BILLY NORWOOD
CISO, FFF ENTERPRISES

ALEXANDER BERMUDEZ
CISO & DPO, FISKER, INC.

THREE STEPS TO ADDRESS REGULATORY CHANGES IN 2023

SOC 2 PREPAREDNESS

MARCH 2023

KLOGIXSECURITY.COM

617.860.6485

TABLE OF CONTENTS

Regulations *March 2023*

FROM THE Editor

Dear Readers,

Regulations have always been top of mind for the security industry, yet with continuous changes and increasing pressure from boards and executives, CISOs are tasked with keeping pace.

In this issue of the magazine we hear from leading CISOs and industry experts about their experience and approach to regulations.

Page 4: Better understand upcoming changes in relation to New York State DFS (NY DFS), California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), and the Securities and Exchange Commission (SEC). Ryan Spelman, Manager Director of Cyber Risk, shared three steps to address these changes.

Page 8: Scott King, CISO, Encore Capital Group talks about how his vast experience in IT and security impacts his ability to effectively communicate with the business and proactively engage with executives.

Page 10: Billy Norwood, CISO, FFF Enterprises discusses his experience building security programs from the ground up, overcoming challenges, and leading a successful team.

Page 12: Alexander Bermudez, CISO & DPO, Fisker, Inc. shares how he leads a team working at an innovative electric vehicle manufacturer. He gives insight into the importance of a secure product development lifecycle and how to integrate security into all business decisions.

Page 14: If you need a refresher on SOC 2 preparedness, Leslie Ogu, Senior Technical Advisory, K logix, shares updates on how to prepare for SOC 2 compliance and key areas to consider.

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.

REGULATORY UPDATES

Three Steps to Address Regulatory Changes in 2023

By Ryan Spelman, Managing
Director, Cyber Risk

Understanding Key Regulatory Changes

2023 brings changes in major regulatory requirements including New York State DFS (NY DFS), California Consumer Privacy Act/California Privacy Rights Act (CCPA/CPRA), and the Securities and Exchange Commission (SEC). While some of these changes may make modifications over the course of the year, no matter how you look at it, this year is going to be monumental for cybersecurity regulations and something every CISO and security leader needs to be thinking about. But more so, the leadership of organizations must spend time understanding what's in store and the business impact once these regulations come into effect.

Why does following regulations matter? Failing to meet regulatory requirements is costly. The average cost of fines for NYS DFS is about $10 million. In October 2022, they fined $4.5 million for failure to conduct periodic risk assessments, together with failure to implement multi-factor authentication and secure access controls, resulting in a breach that exposed New York consumer data. For CCPA/CPRA, the first public fine was $1.2 million due to a failure to comply with injunctive terms. The SEC has fined many organizations, one for almost $500,000 for disclosure controls and procedure violations related to a cybersecurity vulnerability that exposed sensitive customer information.

NYS DFS	CCPA/CPRA	SEC
Average cost of fines is around $10 million	First fine issued was for $1.2 million	Up to $35 million for cyber fines

New York State Department of Financial Services CRR 500

NYS DFS was established in 2017, and the first state-level cybersecurity regulation for financial institutions. It covers all financial institutions regulated by NYS DFS, including mortgage companies, insurance companies, and state-chartered banks.

It is very prescriptive, requiring: naming of a "CISO" or equivalent, cybersecurity policy, penetration testing and vulnerability assessment, risk assessment, and annual Board certification.

New Regulations for NYS DFS Include:

- Tiers of enhanced requirements based on revenue and size of company. If you are a "Class A" company, you must have certain things in place such as audits, password control, monitoring, and an EDR solution. This is the first time an organization has been mandated to have an EDR solution in place.
- CISO independence. CISOs must have an adequate level of independence as it pertains to their authority, oversight, and decision-making.
- Greater Board responsibility. Previous iterations did not include Boards, but now the Board has to approve cyber policies, and have a certain level of cyber knowledge or resources to help show they understand the topics at hand.
- Expanded focus on Business Continuity and Disaster Recovery. This requires significant details regarding designations of certain personnel,

communications and more.

- Tailored Risk Assessments. They are enhancing risk assessment requirements with actual teeth behind what defines a risk assessment.

California Consumer Privacy Act/ California Privacy Rights Act

CCPA was created to avoid a constitutional change in policy and created GDPR-like state privacy requirements in 2018. CPRA was a constitutional change that provides greater clarity and creates an enforcement mechanism for CCPA, taking effect in 2023.

CCPA covers entities that meet any of the following:

- Handle data on over 100,000 California residents
- Has nexus and over $25 million in revenue
- Make over 50% of revenue from data transfer or sale personal data of California residents.
- Requires organizations to implement
- “Reasonable Security”

New Regulations for CCPA/CPRA Include:

- CPRA created the California Privacy Agency (which comes into action in 2023)
- Defined sensitive personal information to include social security number, driver’s license, account log-in, password, and even precise geolocation
- Contractor is defined as a service provider that can provide a “Certification” that it will, among other items, implement security safeguards

The Securities and Exchange Commission

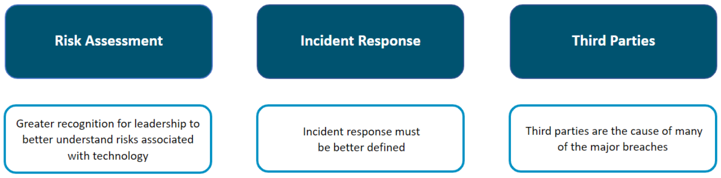
The SEC has shared guidance for boards on disclosing cybersecurity events and has more prescriptive guidance for financial firms. The SEC has broad jurisdiction, and their changes around cyber risk are aimed to be more rigid.

Potential Changes for Public Companies Include:

- Defined policies and procedures
- Clarity on managers role
- Board of Directors oversight and any expertise
- Updates to cyber incident details

There are also changes to regulated advisors that aim to be more stringent with an emphasis on third parties and risk assessment.

Three Common Themes Across Regulatory Changes



Risk Assessment

Incident Response

Third Parties

Greater recognition for leadership to better understand risks associated with technology

Incident response must be better defined

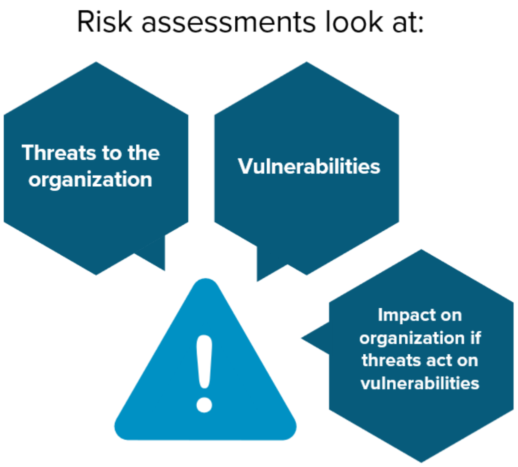
Third parties are the cause of many of the major breaches

To address changes to NYS DFS, CCPA/CPRA, and SEC, key cyber areas must be evaluated and strengthened across organizations. These three themes include risk assessments, incident response, and third parties.

Risk Assessments

Many organizations say they’ve conducted a risk assessment, however what they really did was a gap analysis. Risk assessments must look at threats to the organization, the vulnerabilities in place, and the impact on the organization if threats act on vulnerabilities. It may be mapped to a framework, and it must include a clear prioritization of gaps. Paramount is that leadership across the organization, including the Board, is briefed on prioritized results from a risk assessment.

It is key to determine where threats could potentially infiltrate, then to build out priorities by understanding the gaps and vulnerabilities. It is also important to ask questions like do I have the right change

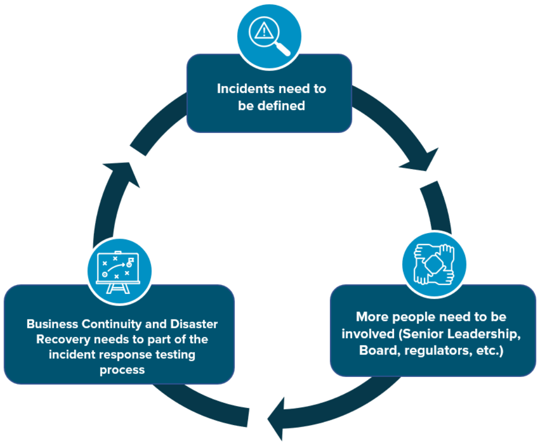

Risk assessments look at:
Threats to the organization
Vulnerabilities
Impact on organization if threats act on vulnerabilities

management? Are the right firewalls in place? Then bringing in a framework, preferably an industry standard like NIST, CIS or ISO, to map controls and determine where vulnerabilities exist. By using a publicly available framework, it is easier to translate across vendors and/or partners. It is vital to know the impact if a threat hits a vulnerability, for example - what happens when a phishing attempt works on a power admin with holistic access? If you know your vulnerabilities and which users have power admin rights, you can now prioritize this as a top focus area.

Regulators are pushing risk assessments so organizations know which vulnerabilities to address, and in what priority order to do so.

Incident Response

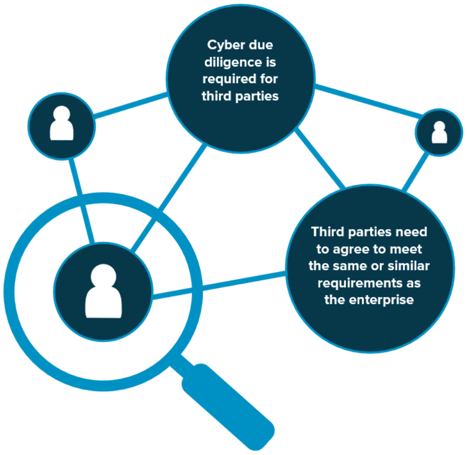
The definition of an incident must be clear and understood across the organization, including the Board. Intrusions or breaches are not incidents, so understanding what an incident means to your organization is crucial. There are different types of incidents each requiring different levels of response. Major incidents might involve the Board and require regulators to be notified, whereas minor incidents may only require internal remediation.


Incidents need to be defined
More people need to be involved (Senior Leadership, Board, regulators, etc.)
Business Continuity and Disaster Recovery needs to part of the incident response testing process

Business continuity and disaster recovery must be part of the incident response plan. Communication between these two units must be fluent and frequent. Incident response exercises and testing should include what would happen if a natural disaster were to occur and parts of organization are shut down. It is important to identify the team members involved on both sides and their individual and shared responsibilities.

Third Parties

To maintain compliance with regulatory changes, third party management must rely on thorough due diligence. Unfortunately, third parties are the cause of many major breaches, causing significant financial, operational, and reputational damage on organizations.


Cyber due diligence is required for third parties
Third parties need to agree to meet the same or similar requirements as the enterprise

How you approach third party due diligence varies and there is no one size fits all, it may range from a straightforward questionnaire to an automated tool that assess risk using external objective data sources. It might be a mix of the two or something like contractual obligations, but either way due diligence must be put in place.

Your third parties must agree or meet similar requirements to those your organization has in place. You are responsible for customer and partner data, and if you share this data with third parties, they must be willing to meet the same or similar level of accordance.

Ramifications if something goes wrong at a third party reflect directly back on their partners and you may be just as liable. Cyber implications around third parties should be understood by senior leadership, the Board and any business units involved vendor decisioning and contracting. There are many different ways to approach this challenge, but you need to have a process, policy, and procedure understanding at all levels of the organization.

How K logix Helps

Keeping pace with changing regulations is achievable when focusing on key theme areas. We work with many security teams looking to bolster and evaluate their approach to risk assessments, incident response and third parties. Our approach is always white glove and focuses on meeting our customers where they are. If you are interested in learning more about our consulting services, let us know: info@klogixsecurity.com.

About the Author

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

Image sources:

NYSDFS image source: https://www.dfs.ny.gov/

CCPA Image source: https://oag.ca.gov/privacy/ccpa

SEC image source: www.sec.gov

PROFILES IN Confidence

SCOTT KING

CISO
ENCORE CAPITAL GROUP

HEADQUARTERS: San Diego, CA

EMPLOYEES: 6,900+

REVENUE: $1.4 Billion

Scott King has worked in information technology and security his entire career, giving him the ability to build up his responsibilities and experience as he progressed in leadership roles. His early jobs were more traditional IT focused roles, working in systems administration and network engineering. His first formal security role was supporting the United States Navy and the Marine Corps as an Information Security Engineer monitoring consoles, watching for malicious activity, and conducting other SOC analyst type duties. Scott explains, “This was back in the early days of information security, and security was somewhat undefined. A lot of the things that we did, we had to figure out how to do on our own. There wasn’t as much training or formal instruction manuals out there. We used our intuition and knowledge to figure out what we’re looking at and how to handle it.”

Along with a multitude of experience across different industries, Scott also has experience working on the vendor side of security, as a Cybersecurity Technical Consulting Lead and a Senior Director Cybersecurity Services for two larger security vendor organizations. He comments, “Because of these vendor side roles I have a really solid understanding of how the vendor process works, how customer success operates within a vendor organization, and how support functions operate within a vendor organization. I now understand that ecosystem at a granular level which really helps me work with the vendor community.”

This widespread experience has enabled Scott to grow professionally, understand the business, and fine tune his communication skills. Throughout his career he has had opportunities to build, run, manage, operate, and lead security organizations. He has had exposure to how security works within sales, marketing and product management departments, along with many other business lines.

Scott currently works as VP and CISO for Encore Capital Group, a publicly traded debt buying organization.

FOCUSING ON CORE SECURITY PROGRAMS TO REDUCE RISK

Scott and his team work across the traditional security program areas, ensuring goals are met and projects are aligned with the business. He explains, “We focus on overall program management, in areas such as project management, activity and task management, as well as our governance, risk and compliance function which facilitates our reporting to our different boards. We also have a security operational element which focuses on things like incident response forensics and 24/7

> “Build relationships and build partnerships with the areas of the organization that are driving the business, because those partnerships and those relationships that you build are vital to your success.”

monitoring around the operation of key security tools and controls that we run through the organization. And then an engineering architecture function where we do things like performing risk assessments of technology, evaluations and integrations with project work whether it's an IT project or a business project. We work to help define what strategic architecture looks like in order to protect our organization as best we can using the technologies and capabilities that we're bringing to the table from our operational capacity."

Scott says there are also shared responsibilities with other business departments. They have a strong partnership with their IT, risk and audit teams, along with other business teams that help facilitate the security function.

His focus for the next 12 to 18 months is addressing the ever-evolving threat landscape. He says, "The biggest focus areas for us is on our preventative capabilities and ensuring that our detective capabilities are working correctly in the way that we would need them to. And then ensuring our responsive capabilities are in place so if something should happen, we're in a really solid position to help recover the business. These focus areas obviously have many legs to them, there's various activities, projects, and efforts that we have underway to help bolster and improve our overall capabilities in those areas."

LEARNING THE BUSINESS TO COMMUNICATE EFFECTIVELY

To effectively communicate with executives, Scott relies on taking the time to learn the business. He explains, "What's unique about a security leader is that they're often given an opportunity to work in different industries throughout their career. And what I would advise is to spend the time to really learn what your business does, how it makes money, how it spends money, how it goes to market, what its core services and offerings are, how it interfaces with its customers, and how it interfaces with its vendors. And I don't mean from a technology perspective, I mean from a core business service perspective."

He continues, "Build relationships and build partnerships with the areas of the organization that are driving the business, because those partnerships and those relationships that you build are vital to your success. And through that collaboration and through that shared interest is where you will help your company be successful."

To ensure these relationships are maintained and matured over time, Scott believes in knowing your audience and orientating security conversations around their goals and challenges.

Scott says by translating security into business risk, security leaders are able to effectively communicate and gain buy-in across the business. Scott recommends tying risk back to revenue or operational cost impact. He says, "Every business model has a run rate. They know how much money they're generating based on operational workloads. And if you can tie back a specific availability concern or risk associated with data integrity or the confidentiality of integrity to a financial metric, you have an informed decision about how that risk stacks up against other risks the business might be impacted by."

LEADING BY EXAMPLE

Supporting his team is paramount to Scott, and he says his goal is to enable them to be successful in their role. He provides guidance to help them both identify and overcome challenges from a holistic perspective. He comments, "I help connect the dots for people. If there's something that we need IT or another part of the organization to work with us on, my job is to make sure we have that lane open for the team so they can do their jobs and they can be successful. And that not only can they be successful in their job now, but they can also position themselves for their future jobs."

To continue to grow and learn as a leader, Scott is an avid reader to keep up with trends like AI and machine learning or understand the latest happenings in the technology world. It helps him stay in touch with the evolution of technology and security capabilities, and provides a deeper appreciation for what's happening in the security industry. He explains, "And then the other thing that I've really found a lot of value in for myself is going through leadership development programs. These help me learn how to be more successful as both a manager and a leader. These help me think differently, develop stronger emotional intelligence, and be more of a level-headed person when addressing challenges."

BILLY NORWOOD

CISO
FFF ENTERPRISES

HEADQUARTERS: Temecula, CA

EMPLOYEES: 1,000+

REVENUE: Privately Held Company

PROFILES IN Confidence

Billy Norwood has over 20 years' experience working across many roles and industries. He joined FFF Enterprises in 2020 as their Chief Information Security Officer. Founded in 1988, FFF Enterprises is a leading supplier of critical-care biopharmaceuticals, plasma products and vaccines. Prior to joining FFF Enterprises full-time, Billy ran his own advisory firm focusing on fractional CISO roles for SaaS firms. He comments, "I was interested to join FFF because they offered a broad product array outside of their distribution business, including software products, SaaS-based products and IoT. So having many different types of products was compelling, along with the strong leadership they have in place."

In his current CISO role, Billy oversees the overall cybersecurity strategy. This spans security architecture and engineering, security operations, and product security, along with shared responsibility for privacy, third party risk, and physical security.

He explains, "I've been here for a little over two years and we continue to mature many areas of our program. I spend a lot of time in security engineering, operations, and product security as the company develops new products. I'm also running risk assessments, doing threat modeling exercises, and focused on addressing privacy. Right now, we have a big push to become CPRA compliant in anticipation of the law going into effect. I've also been working with our General Counsel and outside privacy counsel on areas like our data governance program."

BUSINESS-FOCUSED SECURITY

Speaking in business terms comes naturally to Billy, in the past he owned his own consulting firm and attained his MBA with a focus on entrepreneurship. Having an entrepreneurial spirit gives him a unique perspective that goes beyond a technical focus. He approaches security from a holistic perspective, taking into account security's role in each department, understanding their goals and challenges and how he can leverage security to make a positive impact.

He comments, "To align security with the business I use terms like time savings. I am able to tell executives that if a developer can identify a vulnerability and remediate it before it's in production, we save X amount of time and are less exposed in production. I try to make sure security is known as the guardrails not the gates for the business. If a developer is working on a product, security can identify critical issues up front while they're working on the proof of concept, not once they are almost done with development. As you get closer to QA and production, you start tightening the guardrails down, but you don't want to build a gate at the very end right before they go live, and everyone has signed off."

Many businesses are transforming at rapid paces, not unlike FFF Enterprises, and Billy is tasked with ensuring his team keeps pace while security remains strong and continues to mature.

CONTINUING TO GROW A SUCCESSFUL PROGRAM

Billy's first year was dedicated to building the program from a tooling and hiring perspective. He is now set on continuing to improve key processes around each security program area. Similar to many other CISOs' focus areas, Billy is bolstering their identity and access management program. He comments, "With developers being able to use cloud native technologies and Kubernetes, we want to make sure

> *"I try to make sure security is known as the guardrails not the gates for the business."*

nothing is reaching outside or reaching laterally where it shouldn't be. We are spending more time on the QA portion for security as well as making sure we have threat modeling for new major features ahead of time. So, the focus is on both processes and tools."

When investing in new products, Billy relies on vendors that might offer additional professionals services to help with implementation or quarterly check-ups. Ease of use in deployment is key to save his team time and ensure a smooth transition. Unique to Billy is his past experience working on the vendor-side of security where he gained exposure to how vendors productively partner with organizations and provide a multitude of benefits, especially to security teams with smaller headcounts. He explains, "I've been on both sides of the coin. If you're good to your vendor, they'll be good to you. They'll let you know what's coming out on their roadmap and catch you up early if there's going to be a price increase. If you have a good relationship, they become a partner and engage with you on a regular basis, not just sell you something and leave."

His team is also focused on leveraging automation for speed to close vulnerabilities and address incident response. And similarly, by focusing on orchestration, his team can benefit from things being done quicker with less of a drag on their time.

PARTICIPATIVE LEADERSHIP AND EDUCATION

Billy believes in participative leadership, constantly engaging with his team to build a community and encourage open dialogue. He explains, "I don't draw a hard line that this is my stuff, and this is your stuff. I like to keep them informed. I find if you keep your teams informed about what executive management's talking about, it keeps them very invested in the company. They can see the growth and the roadmap looking forward, and it gets them excited. I like to be collaborative and let them take the first shot even when I might think my way might be better. Worst case scenario, it's a learning experience for them. And best case scenario, they figure out something that I didn't know and it's a learning experience for me. As wide of an area that security is, they might know better than me and teach me something."

Encouraging his team to explore areas they might not be familiar with is also important to Billy. If they are interested in the cloud, they can take cloud classes and get involved in that area of learning. And it benefits the organization because the developers might be working with cloud-native technologies, so his team has broader education to help.

Billy continues, "As part of my team's individual goals, they are given many educational opportunities. They can attend industry conferences or even get certifications if they'd like. Taking classes around their interest area is something I let them decide on. I think it's key for every company to give people the opportunity to continue to learn. It is so easy to get caught up in the day to day tasks, but learning new stuff is important, especially in our industry."

> *"I find if you keep your teams informed about what executive management's talking about, it keeps them very invested in the company. They can see the growth and the roadmap looking forward, and it gets them excited."*

To personally continue to grow and learn, Billy relies on meeting with others across cybersecurity to learn what they have going on, trends they are seeing, and any challenges they are currently facing. He also believes strongly in mentorship. He comments, "I look for mentorship opportunities, both within my field and outside of it. It's great to connect with really experienced CISOs who have been working longer than me, who have seen more. They can help you get through tricky politics you might run into and help ease your frustrations on similar things you are facing. You'd also be amazed at the things you can learn from people outside of your field as well. I've talk to CFOs who helped me understand risk management from their perspective because they're guiding entire companies on risk to keep them making money. You can see with a broader vision and understand why certain things happen and decisions are made at the executive level."

Billy also invests his time in reading, whether it is books about being an empathetic leader or how to mature your cybersecurity program. He is currently reading about building more productive remote teams to continue to evangelize for security and lower the security risk across the business.

PROFILES IN *Confidence*

ALEXANDER BERMUDEZ

CISO & DPO
FISKER, INC.

HEADQUARTERS: Manhattan Beach, CA

EMPLOYEES: 850+

REVENUE: $736 million cash balance at the end of 2022

Alex Bermudez is currently the Chief Information Security Officer (CISO) and Data Protection Officer (DPO) at Fisker Inc., an electric vehicle manufacturer focused on design, sustainability, and innovation.

Alex's career began in Information Technology, first working in an IT support desk role then progressing into opportunities with increased technical exposure and complexity. In the early 2000s while working as an IT systems engineer, Alex had an opportunity to transition into information and technology security, his first official role helping to develop a cybersecurity program while leading a team of security professionals for a large subprime lender in California. Although he had taken on minor security responsibilities in previous roles, he was excited for the opportunity to take on a bigger role and contribute the field. He explains, "My transition into security was a matter of being in the right place at the right time, I went from an IT systems engineer to being an IT security manager, with an opportunity to build out a team and work across multiple security domains including administration, engineering, and architecture."

After growing his security experience within the healthcare, manufacturing, and finance industries as an individual contributor and hands-on manager, Alex moved in larger leadership roles as Director, then Vice President, and eventually Chief Information Security Officer.
After working as Director of Global Cybersecurity Risk Management at Panasonic Avionics Corporation leading enterprise and product portfolio security for several years, he was promoted into the Panasonic Corporation of North America, Vice President and Chief Information Security Officer role. He comments, "I had an amazing opportunity to work with, and alongside, very talented engineers for one Panasonic's largest subsidiaries. During my time with Panasonic Avionics Corporation, they were serving approximately 70-to-80% of the world's airlines, developing their inflight entertainment systems and global communication suites. I had the opportunity to travel the world in support of customer accounts. My was responsible for digital and data risk management across enterprise and product systems."

After spending seven years growing his experience and leadership skills at Panasonic, Alex had the opportunity to join Fisker Inc. He ultimately decided it was a great step forward in his career and presented an exciting opportunity to help shape the cybersecurity and privacy program for an innovative electric vehicle manufacturer.

FOCUSING ON CORE SECURITY PROGRAM AREAS

According to Alex, a strong security program starts with emphasizing core foundational areas. He maintains that by focusing on strong governance with alignment to established frameworks, threat monitoring and response, awareness, supply chain surveillance, and continuous risk assessment, so organizations such as Fisker can achieve their objectives and undergo rapid transformation. He comments, "I strongly advocate for aligning the security program with the business, which must begin with a robust governance program. A governance program acts as a guiding principle and ensures that policy mandates from the executive team are clearly understood and followed. Governance is responsible for defining policy standards and guidelines to support the security program. It also establishes key performance indicators (KPIs) and key risk indicators (KRIs) to measure progress and ensure that the program is effectively reducing risk. By having a strong governance program in place, the security team can make data-driven decisions and confidently demonstrate their value to the organization."

Alex emphasizes the importance of integrating security considerations into all business decisions, and not just treating it as an afterthought. He says that secure product development lifecycles should be followed rigorously, from conceptualization to production and beyond. Whether it is a new cloud-based initiative or the launch of a marketing system, the security team must ensure that security is embedded in every phase of development. This involves assessing potential risks, implementing security controls, and monitoring for vulnerabilities both during and after production. By prioritizing security throughout the development process, you are able to ensure the products and services offered meet the highest standards of safety and reliability, while also safeguarding the interests of the organization and its stakeholders.

REDUCING RISK AND SPEAKING IN BUSINESS LANGUAGE

To ensure security is continually aligned with the business, Alex recommends being persistent and speaking in business terms, so threats and vulnerabilities are clearly understood across the enterprise. By focusing on the same terms, it reduces confusion, and you are not reinventing language every time issues are brought up to the board or executive stakeholders. This creates a universal way to discuss risk across the business, especially as it relates to the threat and vulnerability landscape. He comments, “I firmly believe in establishing agreed-upon methods for discussing risk with other departments within the organization. By doing so, we can provide valuable insights on how we analyze risk and help them make informed decisions based on their risk tolerance levels. This collaborative approach not only enhances risk management practices but also promotes a productive and forward-thinking culture within the business. As security professionals, our role is to educate and inform other departments about potential security risks and the potential impact on the organization’s overall objectives. By fostering a culture of risk-awareness, we can better mitigate and manage risks and ultimately drive the business towards greater success.”

He continues, “As a CISO, accountability is a top priority for me. I maintain comprehensive risk registers and record all decisions made within the business regarding risk. To drive enterprise and product security decisions, I have been an active member of steering committees and ensured that relevant stakeholders, including thought leaders, are involved in the decision-making process. To ensure that all decisions are well-informed and properly documented, I maintain a detailed risk register that is reviewed and updated regularly. By taking this approach, I ensure the organization has a clear understanding of the risks they face, the decisions made to mitigate those risks, and the stakeholders involved in the process. Ultimately, this approach enables us to make more informed and effective risk management decisions, which in turn leads to better overall security posture for the organization.”

TRANSFORMING AT THE SAME PACE AS THE BUSINESS

The nature of Alex’s industry means he must continually keep an eye on changing regulations, while at the same time educating the workforce on the security landscape. He explains, “I recognize that there are always areas for ongoing development and improvement. For instance, we recently attained certification of our Cyber Security Management System (CSMS) for UNECE WP.29 R.155 compliance and it is imperative the team is well-informed and continues to adhere to the highest security standards. To achieve this, it is critical that everyone understands their roles and responsibilities in relation to compliance and risk management. To address this need, we’ve implemented a security education and training awareness program specifically designed for the engineering and software development teams. Through this program, we aim to ensure that every team member is aligned with organizational security goals and understands their role in maintaining compliance. By taking proactive steps to educate and train our teams, we can enhance their security awareness, strengthen our overall security posture, and ultimately better protect the organization against threats.”

> *“I believe in leading my team from the front with a servant-leadership approach. This means I am always willing to roll up my sleeves and work alongside my team, and I would never ask them to do anything that I wouldn’t do myself.”*

Due to the nature of transformation as it relates to the electric vehicle manufacturing industry, Alex says he is continuously looking for ways to improve security in the cloud. He plans to optimize existing technologies while investing in others that will enable Fisker to get a strong handle on rapid changes occurring in the electric vehicle industry. From cloud-based vehicle backends providing software defined functionality to cloud based software distribution to hyper connected vehicles, security technologies like cloud security posture management, cloud workload protection, and XDR, will help enable effective cloud protection processes areas such as threat hunting, monitoring, detection and alerting.

LEADING FROM THE FRONT

Alex says he chooses to lead his team from the front in a servant leader style approach. He explains, “I believe in leading my team from the front with a servant-leadership approach. This means I am always willing to roll up my sleeves and work alongside my team, and I would never ask them to do anything that I wouldn’t do myself. My hands-on approach enables me to provide support and guidance to my team whenever they need it.”

Alex is a highly experienced and skilled Chief Information Security Officer and Data Protection Officer with a strong background in enterprise and product security. He has spent over 20 years in the industry, working with many high regulated and complex sectors such as healthcare, automotive, aviation, and finance. Alex advocates for a strong governance program that supports the security program, aligns the security program with the business, integrates security into all business decisions, and speaks in business terms to reduce confusion. He emphasizes the importance of building and maintaining a strong security foundation grounded in globally recognized standards for excellence and risk management principles. Alex’s expertise and dedication to the security field has helped companies such as Fisker Inc. build a robust security program, protect their digital assets, and maintain trust with their customers.

SOC 2 PREPAREDNESS

Better Understand SOC 2 Compliance

By Leslie Ogu, Senior
Security Consultant, K logix

SOC 2 OVERVIEW

In a world where security is as much a hot topic for organizations as it is a concern, the impeding question has continued to linger on how they can truly protect themselves and their customers. Security is a constantly evolving landscape where threat actors find new methodologies each day to attempt to exploit organizations for the data they protect. For this reason, to safeguard customers and their data, as well as maintain their trust, organizations must show that they have effective and adequate security measures in place. To accomplish this, frameworks are a popular route companies have pursued as means of showing a customer that security is a priority, is kept in mind from the beginning, and is in place. One of the more prominent frameworks is American Institute of Certified Public Accountants' (AICPA) Systems and Organization Controls (SOC) 2.

SOC 2 CRITERIA

SOC 2 is a framework that focuses on controls for an organization to implement based on the Trust Services Categories (TSCs)of security, availability, privacy, confidentiality, and processing integrity. The criteria outlined in SOC 2 provide guidance on relevant areas of cybersecurity that pose the highest risk to organizations and provide insight into other areas of their security program that they should continue to improve. Below is a description of each criterion:

- Security: Measures taken to safeguard information and systems from unauthorized access, as well as potential damage or compromise that could affect the privacy, confidentiality, integrity and availability of the information or systems
- Privacy: Measures taken to manage how personal information is collected, utilized, maintained, disclosed, and disposed
- Confidentiality: Measures taken regarding information that is considered confidential to protect and manage it in an organization's systems
- Processing Integrity: Measures taken to ensure processing conducted by systems are accurate, monitored, timely, complete, and authorized in order to comply with an organization's standards to carry out normal business processes
- Availability: Measures taken to confirm information and systems are available to carry out business functions in compliance with an organization's standards and needs.

PREPARING FOR SOC 2 EVALUATION

To prepare for SOC 2, an organization must define their scope and gather relevant documentation. The American Institute of Certified Public Accountants' (AICPA) Assurance Services Executive Committee (ASEC) outlines the common criteria evaluated in a SOC 2 assessment to give organizations a clear understanding of what must be in place to pass.

These common criteria govern controls pertaining to:

- The control environment
- Information and communication
- Risk assessment

- Monitoring of controls
- Controls activities related to the design and implementation of controls

These criteria evaluate the operating effectiveness of an organization’s controls using the Trust Services Categories (TSCs). The security category is included by default in a SOC 2 assessment. The remaining TSCs of confidentiality, processing integrity, availability, and privacy, are not required for SOC 2. However, organizations should consider incorporating principles from these criteria as they provide additional transparency to customers regarding their security program, and the areas where the organization provides protection. For example, by including availability in the scope, an organization showcases the strength of their business continuity and disaster recovery plans, and processes that will ensure business operate as usual following an incident.

In addition to the common criteria, AICPA provides supplemental criteria that provide increased security assurances deemed critical for service organizations.

These additional criteria govern controls pertaining to:

- Logical and physical access controls
- Systems operations
- Change management
- Risk mitigation

If an organization meets all these criteria, it has covered all security-relevant concerns for all principles within the TSCs.

One helpful measure for an organization would be to delegate a team to assist the different business units in helping the organization understand why SOC 2 is being pursued, executing the necessary preparation steps, coordinate document collection, ensure the business is in good position to proceed with the assessment, and overall, make certain the process runs smoothly.

DEFINING THE SCOPE

With SOC 2, an organization determines how in-depth the assessment will be by defining the scope. This allows an organization to focus on the areas it is strongest to pursue SOC 2.

The drawback of defining the scope is the organization runs the risk of specifying a scope not thorough enough for a customer to develop trust, such as:

- Defining a scope that is too broad:
  - Could consume time and resources needed to create controls for risks that don’t exist in the organization
  - Cause an auditor to discover linked systems or controls that could expand the scope to less secure systems
- Defining a scope that is too narrow:
  - Could mean certain risks will not be identified and this would make the business more vulnerable
  - Result in a report being generated after the assessment that is less useful or beneficial for clients, vendors, etc.

For this reason, it is crucial to solidify a balanced scope that provides enough assurance to customers of the organization’s security controls, as well as confirm the organization’s resources are used wisely.

To help determine the scope, an organization should consider:

- Which TSCs apply to the organization and the services they offer?

- Which systems and documentation support the selected TSCs?
- Which type of report (Type 1 or 2) does the organization desire?

Once an organization confirms their responses, they can finalize their scope and begin collecting the necessary documents to get started.

GATHERING REQUIRED DOCUMENTS

The policies and supporting procedures needed for the SOC 2 evaluation are determined by the scope. All policies and procedures should be established within the organization (i.e., documented, formally reviewed, and approved). If there are processes not supported by documentation, the organization should address this by creating them; otherwise, it will be identified as an exception. For a Type 2 report, evidence must be presented to show the auditor that the organization is following their own policies.

Two additional required documents are the management assertion letter and system description. The management assertion letter will explain the systems used to execute the organization's services, how they are carried out, and how they meet the requirements of the selected TSCs. The system description provides an overview of the organization's infrastructure included in the SOC 2 evaluation. A control matrix is also something that can be provided, and it pinpoints the specific controls that are relevant to the selected TSCs.

SOC 2 EVALUATION

The assessment is carried out by an auditor from a licensed CPA firm that specializes in information security. The auditor will review all documentation provided by the organization, and depending on the type of report being requested, either assess the controls at a point in time (Type 1 report), or the operating effectiveness of the controls over a period (Type 2 report).

SOC II COMPLIANT

ADDITIONAL RESOURCES

Organizations have the option of conducting a SOC 2 readiness assessment that is conducted by an experienced auditor to determine whether their organization is SOC 2 compliant. The organization would receive a letter outlining the gaps that need to be addressed before pursuing SOC 2. Organizations can also take part in SOC 2 audit training to learn more about how to prepare for a SOC 2 evaluation. These resources can be extremely beneficial for an organization to attain SOC 2.

EVALUATION TIMELINE

The average timeframe1 for executing the SOC 2 process is as follows (dependent on the organization's size, selected TSCs, scope, and documentation requirements):

- Getting Organization Approval: ~1 month
- Defining Scope: ~1 month
- Generating Missing Documents: 1 – 3 months
- Collecting Documentation: 1 – 12 months
- Selecting CPA Firm: 2 weeks – 1 month
- Readiness Assessment: 5 weeks – 3 months
- Training: 1 month+
- SOC 2 Evaluation:
  - Type 1: 1 – 2 months
  - Type 2: 45 days – 3 months
- Reporting:

- Type 1: 2 – 3 weeks
- Type 2: 3 – 12 months

SOC 2 COSTS

The average costs for the SOC 2 process are as follows (dependent on the size and complexity of the organization, desired CPA firm, selected TSCs, defined scope, and scope requirements):

- Creating and Collecting Documentation: $3K – $80K
- Readiness Assessment: $10K – $15K
- Training: $2K+
- SOC 2 Evaluation
  - Type 1: $6K – $20K
  - Type 2: $25K – $60K
- Report
  - Type 1: $5K – $10K
  - Type 2: $12K – $20K
- Legal Fees: $5K – $12K

When pursuing SOC 2, preparation is paramount. If an organization is willing to take the necessary measures to prepare for the assessment, they should be in a good position to become SOC 2 compliant.

HOW K LOGIX HELPS

K logix assists customers in understanding security frameworks such as Systems and Organization Controls (SOC) 2, and how they are leveraged to bolster their security program, as well as mitigate successful attacks from threat actors. K logix provides services to prepare organizations to attain compliance for security frameworks, like SOC 2, and create a plan of action to achieve it. With the threat landscape constantly shifting, it is our top priority to ensure organizations are well equipped and well prepared to not only stop tomorrow's attack but protect customers and their data.

ABOUT THE AUTHOR

Leslie has over 13 years' experience in IT and cybersecurity. He is currently a Senior Information Security Consultant at K logix, focused on helping organizations navigate complex cyber risks. Lesie previously held positions at The Internal Revenue Service, George Washington University, The Department of Homeland Security, and Deloitte.

REFERENCE MATERIAL:

Image source: https://www.aicpa.org/
https://secureframe.com/hub/soc-2/audit-timeline
https://cloudsecurityalliance.org/blog/2022/09/15/how-long-does-it-take-to-complete-a-soc-2-audit/
https://www.assurancelab.com.au/resources/post/soc-2-timeline
https://blog.rsisecurity.com/how-long-does-soc-2-compliance-take/
https://www.riskcrew.com/2021/06/how-to-get-soc-2-compliance-and-how-long-does-it-take/
https://secureframe.com/hub/soc-2/audit-cost
https://sprinto.com/blog/soc-2-compliance-cost/
https://www.auditboard.com/blog/soc-2-audit-cost/
https://www.schellman.com/blog/what-does-a-soc-audit-cost
https://www.strongdm.com/blog/how-much-does-soc-2-cost

K logix

1319 Beacon Street
Suite 1
Brookline, MA 02446

617.860.6485
KLOGIXSECURITY.COM

REGULATIONS & COMPLIANCE

FEATS OF STRENGTH
MARCH 2023