Case Study:
How PurePoint International Achieved Compliance for a Financial Services Company

Successfully navigating cybersecurity regulations is no small feat, especially for financial institutions. When a new regulation is passed with a clear timeline to meet compliance, your team needs to be able to quickly pivot in order to meet the requirements.

This is exactly what a New York-based financial services firm faced when the new New York Department of Financial Services (NYDFS 500) Cybersecurity Regulation was passed – giving them only a few months to comply. Unknowingly, the company would also face an upcoming regulatory audit.

In this case study, you'll learn how PurePoint International partnered with a subsidiary branch of a Fortune 200 company to successfully develop and implement a strong cybersecurity posture, maintaining compliance with the new regulations and proving the value of the program to the broader organization.

The Challenge:

While the firm had recognized a need for stronger cybersecurity practices for a while, the primary catalyst for hiring PurePoint International was with the enactment of the new NYDFS 500 cybersecurity regulation. This new regulation required that all New York-based financial organizations not just maintain compliance, but also be able to prove it.

On top of that, the firm's parent-company had just completed a cybersecurity audit, emphasizing the need for a comprehensive cybersecurity strategy. While based in New York, the firm works closely with sister companies based in the United Kingdom, France and Canada which added an additional layer of complexity needing to understand and comply with international regulations as well.

This all led to the ultimate decision to bring on PurePoint International's outsourced Chief Information Security Offer (CISO) services to develop and implement a holistic cybersecurity strategy that kept them in compliance with various regulations, while scaling with the organization.

PurePoint's International's Approach:

Time became a crucial factor in the firm's journey to meet regulatory compliance. PurePoint International was brought on board in January, reporting directly to the General Counsel, and was given authority to make swift decisions in order to meet the March regulatory timeline.

Every engagement with PurePoint International begins with an in-depth onboarding process to get a holistic view of the client's business, high priority needs, and expectations. During this time, we get to deeply understand the people involved –their fears, expectations, and perspectives– in order to craft a truly tailored and unique cybersecurity strategy that resonates with the organization.

In this case, PurePoint International spent every day at the firm's offices getting to know the IT and Operations teams, as well as the firm's international branch based in Paris. This allowed PurePoint International to fully understand the firm's business, regulatory requirements, and expectations. It also allowed PurePoint International to unravel the intricacies of the firm's internal dynamics in order to develop a strong working relationship that would ensure they can meet their goals.

From there, PurePoint International dedicated the next three months to intensive research and implementation to establish a lean, yet effective cybersecurity strategy that ensured immediate compliance with the NYDFS 500 regulation.

Post this foundational phase, PurePoint International collaboratively crafted a 12-month cybersecurity strategy tailored to the organization's specific needs and the expectations of the parent company. A modest budget also prompted PurePoint International to strategically tap into resources from sister companies for optimal outcomes.

> The agreed-upon plan was then diligently executed and led to the hiring of an additional cybersecurity professional–a testament to the tangible value PurePoint International brought to the table.

PurePoint International didn't just stop there. Recognizing the evolving nature of cybersecurity threats, the firm continued its partnership for an additional thirteen months. This phase focused on testing and maintaining the implemented strategy to ensure ongoing resilience against emerging cyber threats and meeting compliance concerns.

Things took an unexpected turn as the firm went through a merger. The Firm's leadership contemplated cutting cybersecurity investments. However, PurePoint International, prepared with compelling messages, convinced executives of the value to move forward as planned. This advocacy not only protected the existing investment in the merger, but supported the regulatory audit that was still to come.

Results:

The impact of PurePoint International's intervention was resounding – not only were they able to successfully meet the compliance timeline for the new NYDFS 500 regulation, but when they were ultimately subjected to a NYDFS 500 cybersecurity audit, they were completely prepared and ready for it.

The audit, conducted on-site, sought tangible evidence of cybersecurity program implementation. PurePoint International's meticulous planning and execution paid off, resulting in a rare, perfect score or "no recommendations back to the business" – an exceptional outcome that validated the entire process.

In a world where cybersecurity standards are relentless, the decision to bring on an outsourced CISO can be transformative – especially for small financial firms like this one. With PurePoint International's expertise and leadership, your company has the ability to not only meet regulatory requirements, but solidify your cybersecurity posture and add tangible value in the face of change.