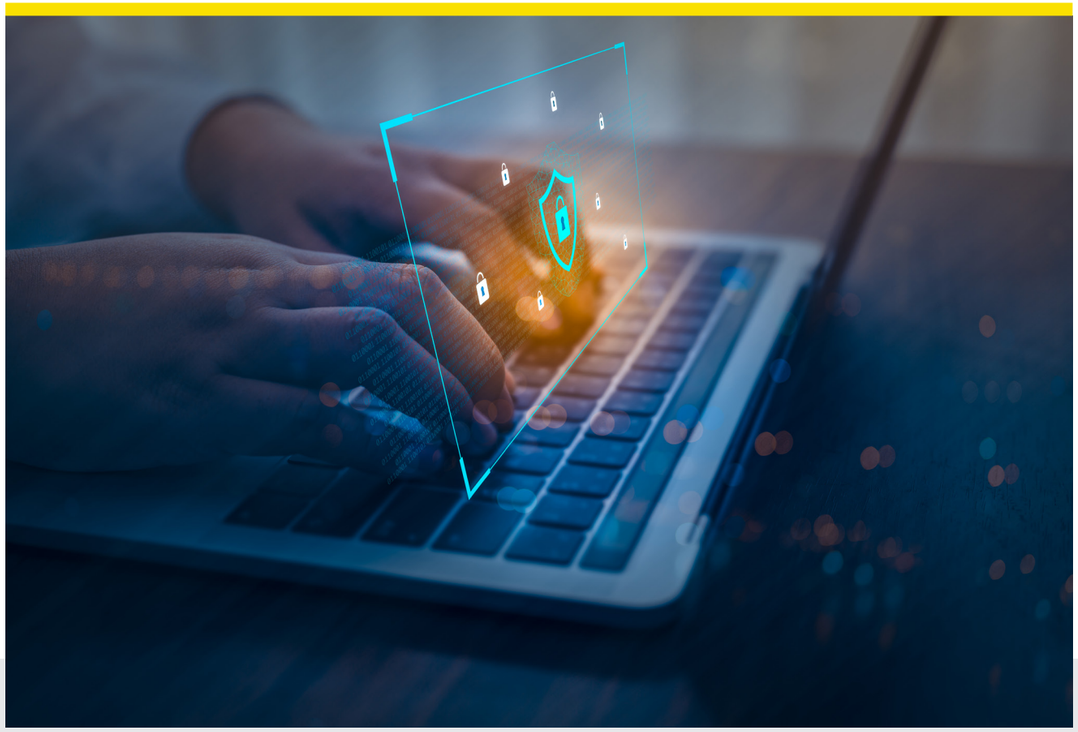
Synechron

POV: Are Cybersecurity Certifications Really Worth It?



Cybersecurity has become a critical priority, especially across the Financial Services industry. Firms often seek different certifications to security standards, and a variety have emerged to prepare the IT staff at companies to create more substantial barriers around each business' data by following new information security standards. But will the emergence of several different cybersecurity certifications be the answer?

We asked two of our cybersecurity experts for their informed opinions. Here's what they said:

Gavin Wilson

Principal Consultant
London, UK

"Even with an established and certified information security management system, senior leadership need to ensure that continued investment and focus is given…"

Achieving certifications can be quite expensive and time-consuming. A business needs to decide if it makes sense to invest the resources to achieve certification versus the business opportunities opened up by having certifications. For large global organizations there are benefits and business cases to achieving certification. For example, if a business wants to trade in Europe, then there is a requirement to comply with GDPR to earn the trust of European customers. Also, ISO 27001 is seen as a gold standard in information security by organizations not just in Europe but across the global. Does a business want to work with governments or healthcare providers? Again, these types of organizations will require businesses to meet specific information security standards/certifications such as CMMC & HIPAA to work in these sectors.

However, over the years we have seen major global businesses who hold multiple certifications (all published proudly and extensively on their websites) fall victim to cyber-attacks. For example, Marriott International (Starwood) was hacked in September 2018, Facebook in April 2019, and LinkedIn in June 2021, etc. So why have cybersecurity certifications if businesses are successfully hacked regardless?

Although having security certifications does not guarantee a business will be immune from hackers, there are still major benefits to implementing information security systems and control. By utilizing an information security standard framework, a business will establish -- at the very least -- a foundation for processes, tools, and people. This can protect the business' Data, Software and IT infrastructure via a defense in-depth solution, across various layers such as physical/building security, Data Management, Web gateways, Email protection, User Training, security policies, and efficient Security Incident response processes. Cybercrime costs global businesses millions of dollars as well reputational damage; a scenario that could be much worse if businesses security controls where not based on Certified information security management system standards.

Even with an established and certified information security management system, senior leadership need to ensure that continued investment and focus is given to ensuring that security controls are up to date and evolving in line with the ever-shifting sophisticated cyber-attacks.

Graham Fletcher

Associate Partner
Greenwich, UK

“Good frameworks and demonstrated competence against them should not be considered as a substitute for active constant analysis of the threat landscape…”

Many security standards and certifications are required in regulated industries where a minimum level of security must be demonstrated. Financial Services and Health Care are good examples of this, e.g., PCI, HIPAA. Independently assessed certifications are a good way of demonstrating to clients that security is taken seriously and that minimum standards are in place and maintained (SOC1&2). Additionally, on the buyer’s side of the same transaction, as third-party provisions of services become more and more common, a standard framework for assessing the security of third-party vendors is valuable.

Even beyond the box-ticking exercise of demonstrating competence, structured frameworks are valuable tools for establishing a good security culture, ensuring that nothing gets missed and raising the bar on controls effectiveness. I personally like the simplicity of the NIST Cybersecurity framework and the intuitive structure of ‘Identify, Protect, Detect, Respond, and Recover’ and they have also developed a wealth of material with specific frameworks for more detailed aspects of security. But often my go-to framework is the CIS Critical Security Controls. This set of controls has been developed over a number of years now and contains an intuitive and structured set of controls specifically designed to protect against known cyber-attack vectors.

As with many things, the framework and any certification that goes with it, only provide a starting point and Cybersecurity professionals need to be able to think outside of these frameworks. The attackers are equally aware of these frameworks and understand that this is how organizations develop their defenses. Consequently, they will be actively looking for attack vectors that dodge the controls in those frameworks.

Good frameworks and demonstrated competence against them should not be considered as a substitute for active constant analysis of the threat landscape and for constantly adapting with innovative ways to anticipate and evade the attacks as they develop.

Synechron’s Point of View (POV) articles explore a key and current topic by way of conveying the informed opinions of our subject matter experts. Agree with one of our experts?

Have an opposing opinion?

Reach out to tell us what YOU think: info@synechron.com

About our SMEs:

Gavin Wilson
Principal Consultant
London, UK

To know more about Gavin
https://uk.linkedin.com/in/gavin-wilson-53302730

Graham Fletcher
Associate Partner
Greenwich, UK

To know more about Graham
https://www.linkedin.com/in/grahamfletcher

www.synechron.com