**Discussion Question: Cryptographic Agility**

Time for a little research. While this chapter describes cryptographic agility, it doesn't really explain how to go about incorporating into the business. Find at least two (2) sources that explain what cryptographic agility is, and best practices for including it in the development process. Summarize each source, and provide an opinion on which source you prefer and why. Include links to each source.

***Before you submit your thread, put your name in the subject line.***

Our book this week touched on cryptographic agility. When researching the concept, I found different websites available, but I ultimately decided to go with an article by Callan on Sectigo and the Zero Trust group on CMS.gov.

According to Callan (2023), crypto-agility means incorporating cryptographic algorithms and practices to handle threats without disturbing normal operations (Callan, 2023). Cryptographic algorithms are evolving rapidly, protecting against the latest security threats (Callan, 2023). Cryptographic practices are pivotal in an organization and are essential for maintaining operations when implementing updates. Callan includes a list of how to achieve crypto-agility; some of these suggestions include having specific guidelines for cryptographic practices and tracking cryptographic elements like “encryption algorithms, digital certificates, and key management systems” (Callan, 2023). Some additional ways are using a PKI for digital certificates and staying current with the latest algorithms (Callan, 2023). Starting policies to adhere to these standards and create role-based access controls are also cryptographic agility practices that should be implemented (Callan, 2023).

According to Zero Trust (2024), cryptographic agility is when a system can alter encryption mechanisms with ease and efficiency (Zero Trust, 2024). If a system is cryptographically agile, it must use the latest cryptography, keep an accurate cryptographic inventory, and help make encryption changes quickly and efficiently (Zero Trust, 2024). Encryption inventories should contain where encryption is used, the algorithm, the key length, and the library of tools for encryption (Zero Trust, 2024).

Both sources touched on information from NIST, adding helpful information to the articles. However, out of the two sources, I prefer Callan’s on the Sectigo website. This is because he provides more robust information on incorporating cryptographical agility into a business.

**References**

Callan, T. (2023, November 10). *What is Crypto-Agility & How to Achieve It*. Sectigo® Official. https://www.sectigo.com/resource-library/what-is-crypto-agility-and-how-to-achieve-it

Zero Trust. (2024). *Three elements of cryptographic agility | CMS Information Security & Privacy Group*. Cms.gov. https://security.cms.gov/posts/three-elements-cryptographic-agility

**Assignment Requirements and Grading:**

1. An initial post of approximately 250 words is due by **Thursday, 11:59 p.m., CT**.
2. For the initial post to be considered substantive, it should be at least 250 words in length and fully cover the topics being presented. Single-sentence definitions or responses will not be awarded points.
3. Submit your post by clicking on the **Assignment Link** above, then **Create Thread**. You must create a thread in order to view your peers' posts. Tip: Create your post in a Word document and then copy and paste your work into the thread.
4. A minimum of three (3) responses, **to the original threads of other students**, of 100-200 words each are due by **Sunday, 11:59 p.m., CT**.
5. To view the rubric grading criteria, click on the following link: [Discussion Board Grading Rubric](https://content.bellevue.edu/cst/csd/rubricdbv3.pdf).

**(50 points)**

Hey, Samir. I enjoyed reading through your summaries of the articles that you included on cryptographic agility. I also thought your post, in general, was very well-written. The web is filled with different articles, so finding credible ones that work best for you can be a game changer in achieving a better understanding of secure software and any topics in general. I like how your sites were not based in the same countries. Having an understanding of different security standards or definitions by country can be vital when working internationally. It sounds like you cannot go wrong with either of your sources.

Hi, Truman! From the sounds of it, you found two great sources to reference for this discussion. Both sources accurately describe how cryptographic agility works. Based on the information we read, it is clear the importance of cryptographic agility. Systems need to understand how to encrypt without corrupting the system in place otherwise major errors will occur. I definitely found it difficult to rate the websites because both had very good information, so I understand your struggle. Based on everything we have learned, I think businesses should focus on crypto agility and have a dedicated developer in place to handle it.

Hello, Joe. I think you did an excellent job on your post for this week, and analyzing your chosen sources on cryptographic agility. I thought it was helpful to better comprehend cryptographic agility since each resource had a slightly different definition. Hearing a concept in multiple ways helps make a concept easier to grasp. I also read through Callan’s article on Sectigo, so it was interesting reading your summary compared to mine. Implementing the company standard is a great way to ensure cryptography agility is successfully integrated. It was interesting that you also liked the Sectigo article better than your other one by Gillis.