NIST
Cybersecurity Framework Success Story
Cimpress

The voluntary Framework for Improving Critical Infrastructure Cybersecurity was developed through a collaborative process by industry, academia, and government stakeholders. It enables organizations – regardless of size, sector, degree of cybersecurity risk, or cybersecurity sophistication – to apply the principles and best practices of risk management to improve security and resilience. NIST does not validate or endorse any individual organization or its approach to using the Cybersecurity Framework.

Organizational Profile

- Cimpress' 14,000 employees work in over 45 countries. The company consists of 17 businesses in the printing, embroidery, promotional products, gifts, home-décor and personalized fashion industries – part of the "Mass Customization" market.
- Cimpress Security, which is a centrally managed function at Cimpress, provides policies and standards for all Cimpress lines of business, while allowing each business to operate independently. Additionally, Cimpress Security delivers products and services through a managed security service provider (MSSP) model.
- Each line of business employs various technologies for its e-commerce and manufacturing, operates in different geographies and markets, and often has industrial technologies as well as more modern e-commerce.

Situation

- Cimpress defined cybersecurity as one of its strategic capabilities. That allows lines of business to operate independently while meeting Cimpress' security goals.
- The decentralized nature of how Cimpress runs required a common framework that would scale from small businesses of a few dozen employees to businesses with thousands of employees, as well as multiple factories and customer call centers.
- Cimpress chose the NIST Cybersecurity Framework (CSF) for its simplicity and adapted it to address requirements for measuring and reporting security maturity.

Process

- To establish a comprehensive, actionable security program, Cimpress decided to combine the qualitative approach of the CSF with quantitative risk analysis based on the FAIR (Factor Analysis of Information Risk) model.
- Cimpress created a self-assessment questionnaire for its business units in order to gain insight into the current state of their security program.

"Taking more risks is only possible when you can accurately and consistently measure it. Utilizing CSF and FAIR allows us to get a clear understanding of our risk and security maturity and direct our risk management in a reasoned fashion."

Ian Amit, Chief Security Officer, Cimpress

Process (Cont.)

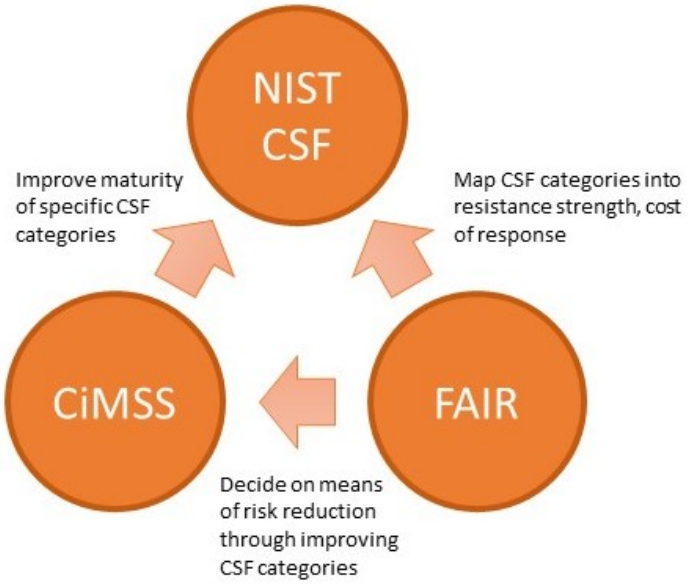
- The questionnaire tailored the Framework Core, removing some subcategories based on Cimpress' needs. Implementation Tiers were adapted to create a maturity model to measure how the Framework subcategories are implemented across business lines. For example, Cimpress excluded critical infrastructure items, and added the business's capability regarding cyber Governance, Risk and Compliance and risk tolerance, as this is a central function for Cimpress Security.
- The self-assessment informed a baseline created to align internal security policies across Cimpress to the CSF and identify maturity metrics. Having this information centralized across the lines of business enables Cimpress to more easily compare businesses and identify gaps.
- Maturity scores were then mapped to FAIR resistance strength scores and used in loss scenario analyses for each business. The FAIR score represents the organization's ability to thwart attacks for the scenario being evaluated.
- By mapping to FAIR resistance factors, Cimpress can provide increased confidence that control/resistance strength is relevant and proportional to the loss scenarios. Additionally, as risk scenarios were evaluated, the risk management staff could more clearly see how investing in increasing maturity would impact the expected losses related to each scenario.
- That turned the process into a highly measurable one that can be more easily justified in terms of budget allocation and risk tolerance. For example, if increasing

the maturity level of the CSF's PR.DS-6 (integrity checks for firmware) would yield a reduction in the expected loss for a factory related scenario of $540K, and the cost of the increase in maturity is annualized at $120K, it would make sense to invest in these checks and keep monitoring the scenario analysis each year.

- Ongoing evaluation processes call for updating the maturity scores of the businesses over time. Those revised scores trigger updates to the FAIR models, which in turn provides a measurable risk-tolerance view for the businesses in financial terms.
- To provide businesses with actionable ways to address their risk, Cimpress Security developed a catalog of managed security products and services, which is available to internal customers.
- Businesses are responsible for addressing maturity gaps. They do that by using services and products from Cimpress Security or outside providers. These actions are reflected in improved maturity scores.

Results and Benefits

- Following implementation of the Cybersecurity Framework and FAIR, and by creating internal MSSP capabilities, Cimpress was able to retain the advantages of a highly decentralized operation while allowing more transparency into its security across all businesses.



Results and Benefits (Cont.)

- Additionally, the company's businesses and corporate management have a better understanding of the impact of risks and can make more informed decisions around managing risk. As a result, Cimpress was able to:
  - Clearly define a minimal maturity baseline for a set of categories for its businesses.
  - Create a clear and common language for evaluating security maturity across different domains.
  - Easily identify improvement areas for each business based on operating environment and threats.
  - Enable self-reporting/assessment with minimal need for security expertise.
- Cimpress plans to continue improving how it uses both frameworks as it automates more elements of collecting and analyzing metrics. The company's goal is to empower stakeholders to make better informed decisions around risk. Cimpress Security will continue leveraging FAIR to evaluate current and future risks and the CSF-based self-assessment tool to manage that risk.

Contact Information & Resources

- Cimpress Website: https://www.cimpress.com
  Cimpress Contact: security@cimpress.com
- FAIR Institute Website: www.fairinstitute.org
  FAIR Institute Contact: info@fairinstitute.org
- NIST Cybersecurity Framework Website:
  https://www.nist.gov/cyberframework
  NIST contact: cyberframework@nist.gov