IN THIS ISSUE:

FDIC Selects GRF & TrustMAPP Team as Winner in Effectiveness/Impact Category of Technology Competition

A Global Resilience Federation led team, including TrustMAPP, was awarded most "Effective/Impactful" in the FDIC tech sprint competition, "From Hurricanes to Ransomware: Measuring Resilience in the Banking World."

GRF presented the Operational Resilience Framework, coupled with a TrustMAPP security assessment that, together, can help measure and improve an organization's resilience to destructive attacks and adverse events.

The "sprint" refers to the short period of time teams had to turn ideas into impactful tools and concepts. Once the FDIC posed the challenge, teams used their collective capabilities to address the scenario.

The FDIC competition evaluated solutions from six teams, reviewed by a panel including representatives from FDIC, the Office of the Comptroller of the Currency, the SEC, Department of Homeland Security CISA, and NIST.

GRF's Operational Resilience Framework is being developed by GRF's Business Resilience Council (BRC) alongside a multi-sector group of security practitioners working to reduce operational risk, minimize service disruptions and limit systemic impacts. The framework will include rules, a reference architecture and implementation tools aligned to standards and existing vendor solutions to ensure the immutable and recoverable nature of data, systems, networks, applications and configurations. Read more about this award.

ORF-Path to Operational Resilience

1 Build a Foundation → 2 Understand Ecosystem → 3 Inventory & Priority → 4 Impact Tolerance → 5 Preserve Data Sets → 6 Enable Recovery → 7 Test & Evaluate

Path ID	Path Description	Rule Topics
1	Implement an industry-recognized **IT and Cybersecurity control framework**.	Security Controls, Sponsorship, Data Governance, Sustainability, Change Control
2	Understand the organization's **role in the ecosystem.**	Counterparty Identification, Counterparty Prioritization
3	**Inventory business processes**, systems and data sets and designate them as Operations Critical, Business Critical and Business as Usual.	Inventory, Criticality, Dependencies, Third Parties
4	Define the organization's **Impact Tolerance** for disruption to each Operations Critical service.	Impact Tolerance, Operations Recovery Objectives, Data Restoration Objectives
5	**Preserve the Data Sets** necessary to support Operations Critical and Business Critical services.	Data Preservation, Immutability, Integrity, Availability, Frequency, Composition, Format, Retention, Non-Production Environment, Deletion
6	Implement processes to **enable recovery and restoration** of Operations Critical and Business Critical services within acceptable impact tolerances.	Operational Resilience Plan, System Recovery and Reconstitution, Secure Transfer, Key Management, Access Redundancy, Recovery Environment
7	**Independently evaluate** design and test periodically.	Independent Testing, Management Exercises, Third-Party Evals., Compliance, Testing of Communications, Technical Mechs, Continuous Improvement

Community Updates and Upcoming Events

Energy Analytic Security Exchange (EASE) Joins GridEx
In November, Program Manager Tim Chase represented EASE in the biennial national electrical grid security exercise GridEx. Tim participated alongside the New York Power Authority as a supporting third party in time of emergency. The two-day event created security scenarios and forced participants to implement mitigations, while challenging assumptions that particular assets and capabilities would be operational. Several practical lessons were learned that will be applied in the EASE strategic plan for 2022.

Cross-Sector Member Calls
The EASE community is also preparing to engage in new cross-sector member calls with many GRF affiliated ISAC/ISAO analysts and members. The calls will allow cross-pollination of ideas and best practices from multiple sectors. A schedule for the call series is forthcoming.

K12 SIX RELEASES CYBERSECURITY STANDARDS FOR SCHOOL DISTRICTS

Developed by K12 IT practitioners, for K12 IT practitioners—and aligned to cybersecurity risk management best practices—the K12 SIX-recommended protections are designed to defend against the most common cyber threats facing school districts, including those recently identified by the Federal Bureau of Investigation (FBI) and the Cybersecurity & Infrastructure Security Agency (CISA). The standards consist of a dozen actionable and pragmatic cybersecurity controls—grouped into four categories—that every school district should strive to implement this school year. Related products include a self-assessment tool, detailed how-to's to assist with implementation, and much more. To learn more visit www.k12six.org or contact Doug Levin.

UPCOMING EVENTS

K12 SIX - December 10, 2021 at 2pm CT K12 SIX webinar, 'Meeting the K12 Cybersecurity Challenge,' in partnership with the Missouri School Boards Association.

December 15, 2021 at 12pm ET **K12 SIX** Member Meeting. Contact Doug Levin for info.

BRC - December 15, 2021 at 2:00pm ET BRC Member Meeting. The agenda and invitation for that meeting will be announced in the coming week.

GRF COMMUNITIES AND CONTACTS
OT-ISAC (John Lee)
LS-ISAO (Raquel Santiago)
EASE (Tim Chase)
ProSIX (Mark Orsi)
K12 SIX (Doug Levin)
BRC (Chris Denning)