INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS

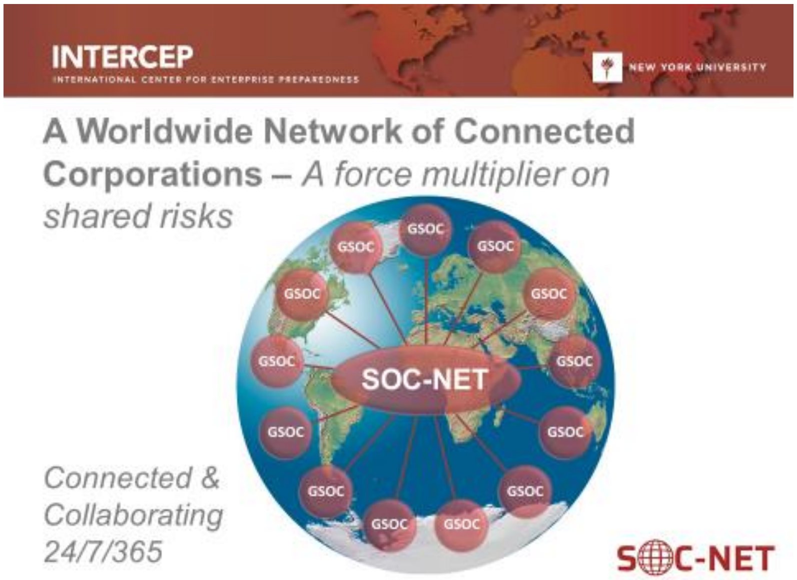
NEW YORK UNIVERSITY

Overview of Technology Need & Context

INTERCEP – Host Center at NYU: The international Center for Enterprise Preparedness (INTERCEP) is a 15 year old center at NYU that focuses on bringing together diverse stakeholders to collaborate on shared threats to their organizations. The Center has strong outreach to and to build the public and private sectors with a strong emphasis on multinational corporations.

A key program of the Center is the Security Operations Collaboration Network (SOC-NET).

SOC-NET – A Program of INTERCEP:



INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS
NEW YORK UNIVERSITY

A Worldwide Network of Connected Corporations – *A force multiplier on shared risks*

Connected & Collaborating 24/7/365

SOC-NET

- Mission: Multinational corporations cooperate to
  - Share operational intelligence on joint threats to their people and operations globally
  - Share best practices and lessons learned on security operations
  - Collaborate on common challenges.
- Approximately 30 major multinational companies participate and growing
- Job titles include: Chief Security Officer, Enterprise Security Manager, Senior Vice President of Intelligence, Crisis Manager, Director of Global Corporate Security, Director of Threat Intelligence, etc.
- A distinctive element of this is that it focuses on connecting the Global Security Operations Centers (GSOCs) of participating corporations. These centers generally consist of one or more analysts who monitor the overall operations of the corporation across the global footprint of the firm. They monitor various data feeds from corporate operations as well as various general news and social media. One core objective is to identify disruptions as soon as possible so appropriate response and recovery activities can be undertaken.

The Near Term Need:

- SOC-NET members have requested the capacity to vet / confirm early threat reports or developing incident information (bombing, shooting, other disruptive events) where members of the community can share a report and its source for others to validate / augment / dispute optimally from alternate sources.
- In addition to vetting information during evolving events, SOC-NET members discuss best practices on various topics – vendors, hiring practices, protocols, etc.

- The current email distribution approach for SOC-NET members may result in substantial volumes of e-mails in personal inboxes.
- A real-time communications platform would reduce the amount of e-mail traffic in personal inboxes.

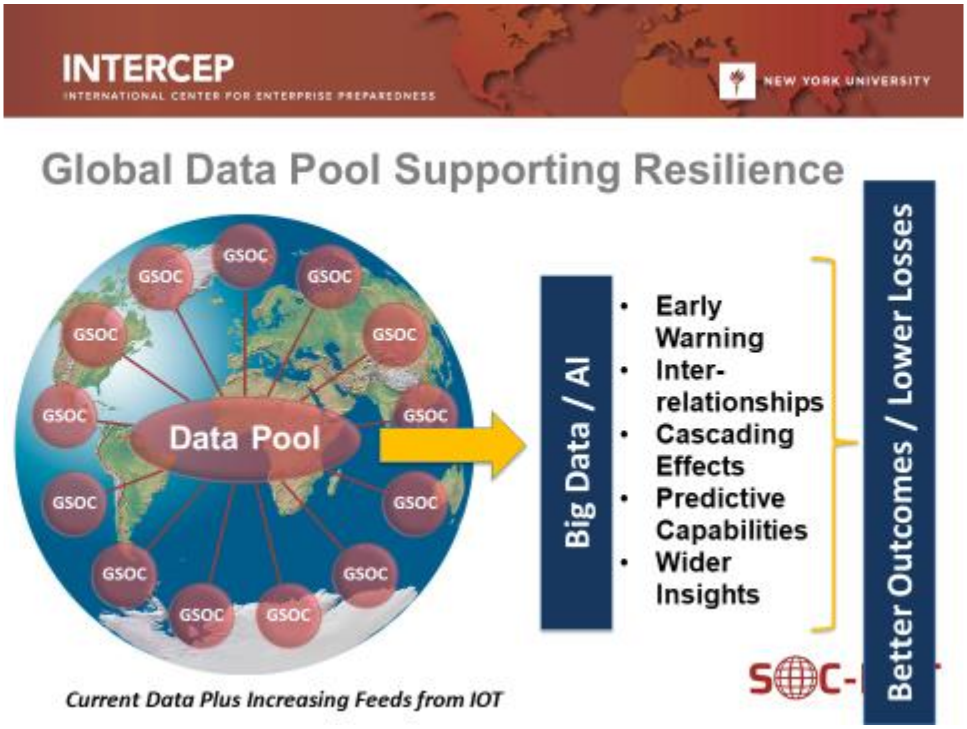
The Concept: Developing the capacity for various data and functional platforms to share data easily through a "translator" capacity. Such a capacity may but need not solely to use web hooks and other elements. They could link platforms such as Microsoft Teams, Slack, ServiceNow. The capacity may also take data in one format and translate it to a generic format which is not only capable of being translated to another platform but this format may be usable for other applications as is.

Potential / Optimal Specifications:

- Users from multiple organizations with different e-mail domains
- Secure (heavily encrypted)
- Single sign-on capability
- Dashboard based online environment as well as friendly to mobile
- Ability to save / archive discussions for future reference
- Ability to start easily start distinct discussions for specific events and topics
- Duality of incident specific, fast-evolving conversations, as well as best practice discussions (longer-form threaded discussions)
- Customizable alerting – ideal would be to have an e-mail sent to all users when a new discussion / topic / thread begins

Long Term Vision

Each corporate GSOC has a diversity of data feeds informing its monitoring role. These data feeds will likely grow dramatically in the near future as the Internet of Things widens. As a trusted third party, NYU INTERCEP could pool this data and anonymize it utilizing various big data strategies. This data pool could then be analyzed via artificial intelligence including machine learning. Such

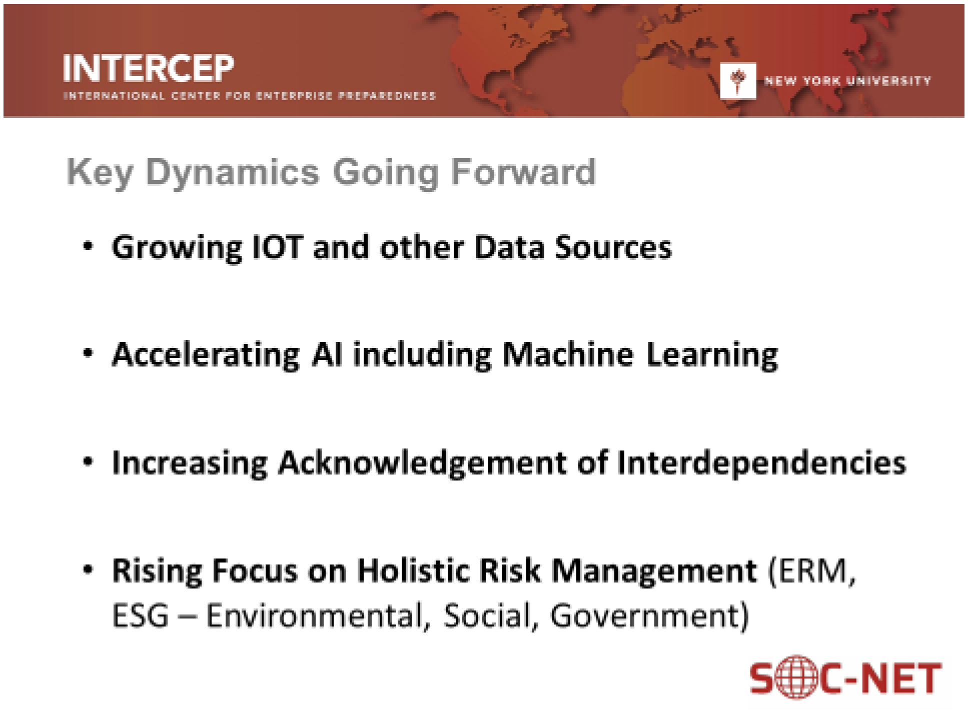

INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS
NEW YORK UNIVERSITY

Global Data Pool Supporting Resilience

- Early Warning
- Inter-relationships
- Cascading Effects
- Predictive Capabilities
- Wider Insights

Current Data Plus Increasing Feeds from IOT

AI application could yield many benefits including earlier warning and faster vetting of disruption reports and a better understanding of interdependencies of both internal and external operations as well as the cascading effects / impacts of those relationships when disruptions occur. Additional insights are also likely including a better understanding of what strategies to address various disruptions are most successful. All this information could further inform more targeted investment as well as incentivization of more effective preparedness, response and recovery strategies to achieve optimal organizational resilience. The ultimate outcomes could be reduced loss of life, minimized disruptions to organizations and a safer and more secure wider society.



Key Dynamics Going Forward

- **Growing IOT and other Data Sources**
- **Accelerating AI including Machine Learning**
- **Increasing Acknowledgement of Interdependencies**
- **Rising Focus on Holistic Risk Management** (ERM, ESG – Environmental, Social, Government)

SOC-NET

For additional information, contact:

Bill Raisch
Executive Director
International Center for Enterprise Preparedness
New York University
William.Raisch@nyu.edu