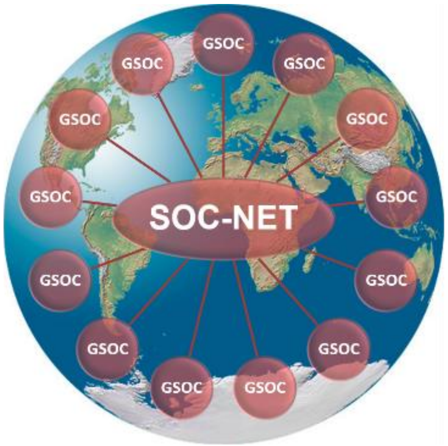
INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS

NEW YORK UNIVERSITY

SOC-NET



SOC-NET Mission: Establish the first global network of continuously connected multinational corporations to collaborate on safety, security and business resilience. The network focuses on:

1. **Operational intelligence on current incidents and future threats** - real time sharing and fusing of information among dozens of corporations across the globe
2. **Best-in-class practices and lessons learned** - sharing of best strategies, policies, procedures and insights from leading corporations to assure the most effective and efficient operations
3. **Coordination of activities & resources** - leveraging collective resources and joint action in blue skies and in crisis – for the benefit of the member corporations, their people and the communities they operate in.

What is different about SOC-NET?

- **Formal GSOC-to-GSOC Connectivity on a 24/7/365 basis**
- **Global Focus** - not regional, domestic or industry specific but still advancing a “Network of Networks” through collaborative approach to other efforts
- **Trusted and Confidential Community** of security professionals under the Chatham House Rule
- **Non-Governmental / Non-Commercial** / **Neutral Ground** convened and hosted by an international university without political jurisdictions or commercial concerns
- **Central Staff Support** to assure focused and ongoing advancement from INTERCEP - no uncertainties of informal voluntary support by varying members

SOC-NET Core Activities & Ongoing Products

- **Real Time Incident / Threat Queries:** Terrorism, severe weather, earthquakes, etc.
- **Best Practice Exchanges / Benchmarking Surveys:** Escalation protocols / triggers, integration strategies, duty of care, GSOC staffing recruitment, training, retention, compensation, etc.
- **Quick Reference Summaries of Best Practices & Lessons Learned Weekly:** Anonymized and summarized from discussions at In-Person Meetings, Monthly Member Web Forums, Surveys and Email Discussions
- **Member Technology Information Database:** Members’ due diligence and experiences with vendors and technologies on situational awareness, integration platforms, weather monitoring, people accountability, video management and analytics, alerting, social media monitoring, etc.
- **Expert Briefings & Member Forums:** In-person Quarterly Member Meetings with GSOC tours, Informal Networking Monthly Member Web Forums, Threat Briefings, Hot Washes / After Action Discussions
- **Curated Contact Base for Immediate Connections to the Member Network:** Security Operations Management and Analysts – emails, telephones
- **Web-Based Member Resource Hub:** Password-access only to Best Practice Summaries, Lessons Learned, Member Contacts and other references
- **Information Sharing Platform in Development:** Evolving alternatives to our current email communications with a more focused and less “noisy” info sharing platform to avoid taxing our inboxes as the network shares more information

NYU International Center for Enterprise Preparedness
Tel: +1-646-997-4020 Email: intercep@nyu.edu Web: www.INTERCEP@nyu.edu

SOC-NET Value Proposition

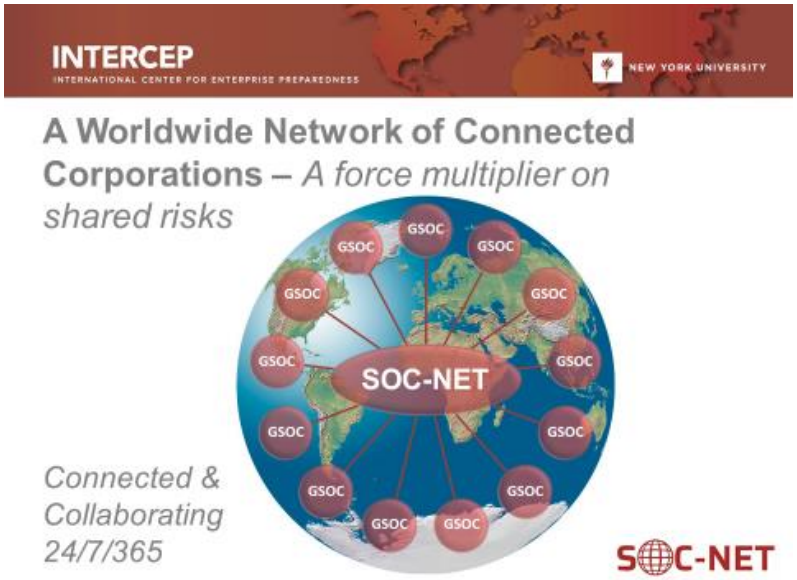
- **Protects the Firm's People**
  - Assuring that the firm is performing its duty of care by integrating the current best practices of the world's leading corporations through ongoing benchmarking and sharing of policies and procedures
  - Real time connections to security operations of leading firms allows for faster identification and validation of threats to the safety and security of employees
  - Earlier notification provides more time for employees to take appropriate action
  - Sharing of best practices enables the development of the most effective safety and security strategies for the protection of employees
  - The ability to collaborate with other companies on response and recovery from emergencies provides greater resources and capabilities to help our people in crisis
- **Protects the Firm's Property & Processes**
  - Identifying and better understanding future threats through the collective input of dozens of global corporations allows the firm to take action in advance to avoid or minimize the impacts of potential threats to the property and operations of the company.
  - Earlier identification and member-to-member confirmation and additional information on emergency incidents allows for more timely response which can avoid or minimize disruptions to business operations and loss of property.
  - Benchmarking with leading firms on security, continuity and resilience practices allows for the development of best-in-class strategies to assure the most effective response to and recovery from disruptions when they occur thereby minimizing damage to property and disruption of operations.
  - Sharing of due diligence and experience with technologies and vendors through the SOC-NET technology database supports both the selection of appropriate technologies as well as the optimal application of that technology to the firm's needs.
- **Protects and Enhances the Firm's Reputation**
  - Reputations built over decades can be damaged in moments, especially when appropriate actions are delayed or inappropriate actions are taken.
  - SOC-NET supports earlier identification of both real time incidents and future threats which allows for action in advance to avoid or mitigate threats that could impact reputation.
  - The ability to quickly compare potential response actions with other firms in emergencies assures confidence in taking your firm is taking the appropriate steps.
  - Participation in the SOC-NET network demonstrates that a firm regularly benchmarks its practices with leading global firms to assure best-in-class security and business resilience practices to address potential concerns in the aftermath of any event that the firm was not for appropriately prepared.
- **Protects and Sustains Revenue**
  - Avoids some disruptions to operations / maintaining revenue (through more robust intelligence sharing on current and developing future threats)
  - Minimizes other disruptions to revenue (through earlier notice and confirmation of incidents as well as improved planning through access to best-in-class practices)
- **Lowers Expenses**
  - Lowers recovery costs (through improved preparedness, lesser incident impacts and shorter recovery periods from best practice sharing)
  - Lowers technology costs through the member technology info exchange (leveraging experiences of other members on technology and vendor experiences)
  - Lowers staffing related costs (shared practices on recruitment, retention, and compensation)

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.

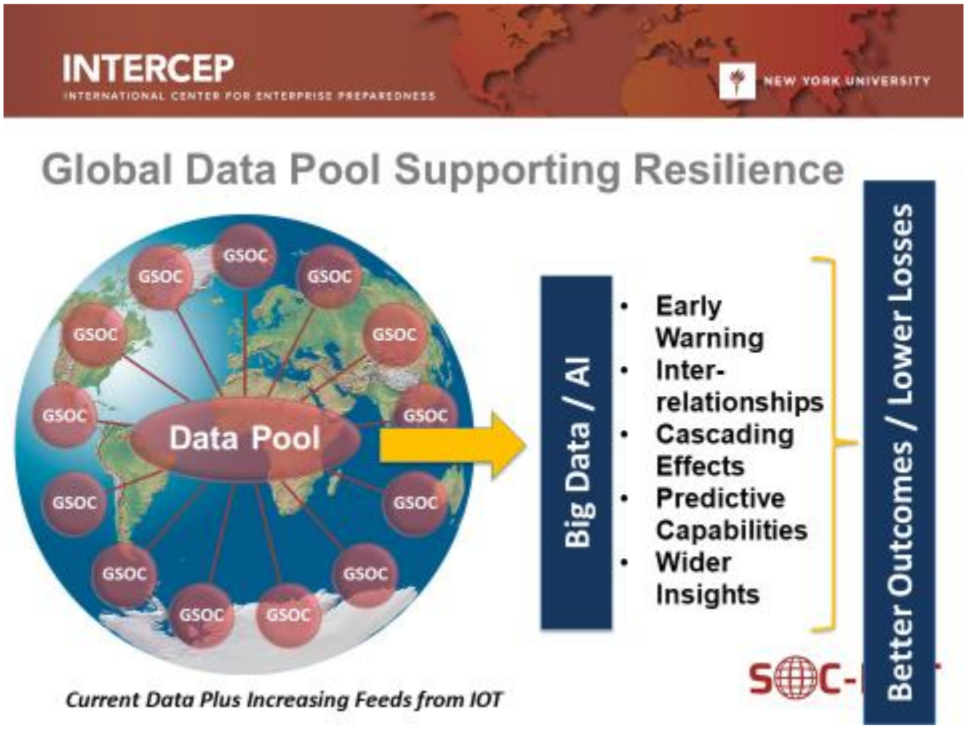
The Concept: Developing the capacity for various data and functional platforms to share data easily through a “translator” capacity. Such a capacity may but need not solely to use web hooks and other elements. They could link platforms such as Microsoft Teams, Slack, ServiceNow. The capacity may also 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



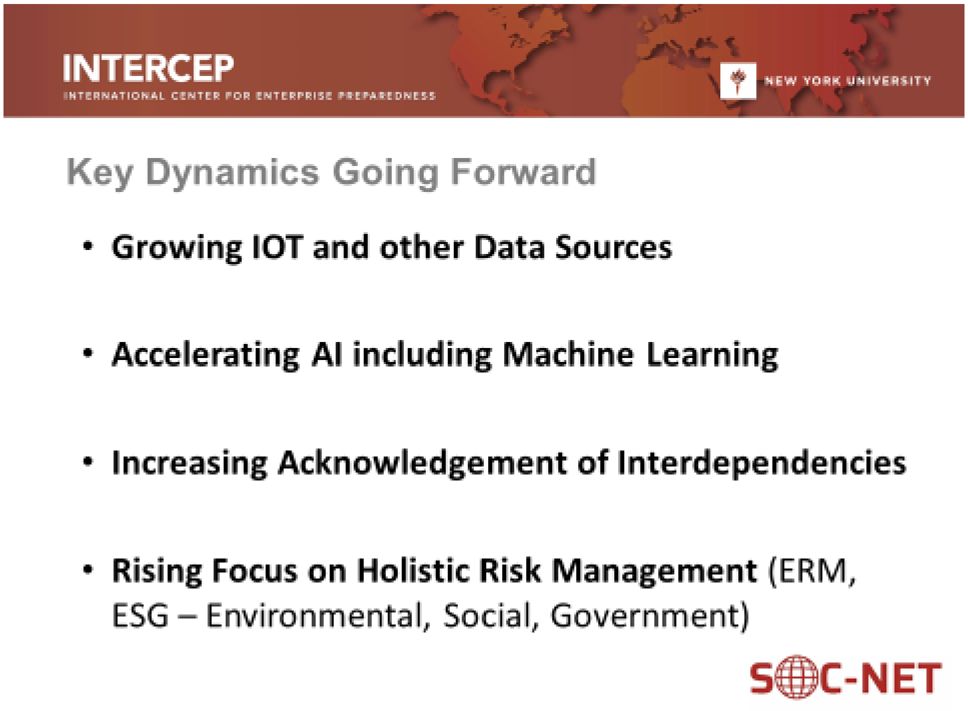
INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS
NEW YORK UNIVERSITY

Global Data Pool Supporting Resilience

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

Better Outcomes / Lower Losses

Current Data Plus Increasing Feeds from IOT



INTERCEP
INTERNATIONAL CENTER FOR ENTERPRISE PREPAREDNESS
NEW YORK UNIVERSITY

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

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.

For additional information, contact:

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