RANE

Risk Assistance Network + Exchange

RANE Cybersecurity Program

- The RANE Approach
- Program Details
- SEC Checklist
- RANE Case Study

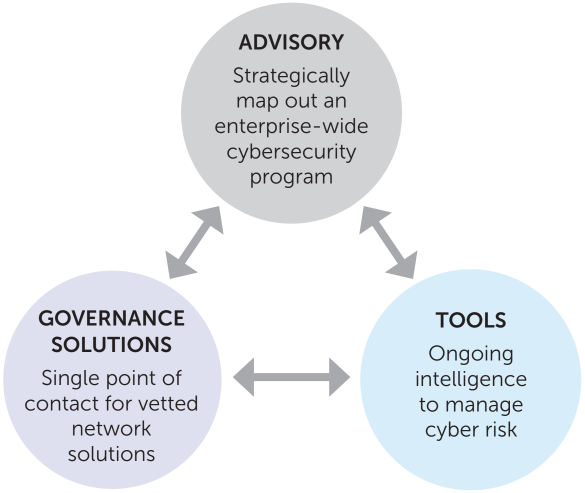
THE RANE APPROACH

The cyber threat to companies is not a regulatory or technology issue—it's an enterprise-level **corporate governance** issue. As such, strong risk management controls are critical to ensuring that information about cyber risks and incidents reaches senior management, the board, and investors.

RANE's program includes:

- **Advisory services to map out and implement an enterprise-wide cybersecurity program**, with active and ongoing stewardship by RANE subject matter experts.
- **A range of cyber governance solutions**, with the ability to tap into a global network of credentialed cybersecurity service providers to save you time and effort.
- **Tools that provide ongoing intelligence to manage cyber risk** and keep pace with emerging threats, rapidly advancing technology, and the latest regulations.

Cybersecurity Program Framework


ADVISORY
Strategically map out an enterprise-wide cybersecurity program
GOVERNANCE SOLUTIONS
Single point of contact for vetted network solutions
TOOLS
Ongoing intelligence to manage cyber risk

The RANE Approach

RANE's comprehensive program leverages our in-house experience combined with access to a global network of cyber experts and service providers.

Cybersecurity as a corporate governance issue
Strategic analysis and recommendations to ensure up-to-date policies, procedures, and controls.

Focus on cyber resiliency and preparedness
Access to world-class cyber experts and information on cybersecurity risk, technology advancements, and regulatory trends.

Active and ongoing stewardship by RANE subject matter experts
A provider-agnostic partner to help you navigate the cybersecurity landscape.

SAMPLE PROGRAM: Year 1 focuses on building out your program; Year 2 focuses on maintaining it

Initial assessment with gap analysis and roadmap for execution on cybersecurity program.

On site support for deploying and training employees throughout execution of roadmap.

Review procedures and personnel involved in updating policies to comply with regulations; establish preliminary framework and cadence for informing senior leadership.

Complete review of all cybersecurity focused vendors to ensure they are aligned with organization's level of sophistication.

Refine reporting framework for informing senior leadership of cybersecurity protocols and program.

Ongoing: Information tying together implications of current and impending cyber regulations, cyber threat landscape, and technology.
Ad-hoc research support on cybersecurity issues.

PROGRAM DETAILS

RANE's modular approach provides you with the flexibility to customize a program specific to your needs.

ADVISORY	GOVERNANCE SOLUTIONS	TOOLS
Cyber Assessment, Gap Analysis, & Roadmap Comprehensive assessment and deployment plan covering legal, policy, and technical aspects of cybersecurity with roadmap for execution on where to invest time and resources.	**Data Management** Perform data identification, mapping, compartmentalization, and classification. Assist in selecting products for data governance	**Regulatory Guidance** State, federal, and international regulatory guidance, trend analysis, and interpretation related to cybersecurity, including suggestions for compliance.
Information Security Policy Review of current policies and written recommendations. Best practices on how to disseminate the policy to workforce and training techniques	**Incident Response Plan & Tabletop Exercise** A written plan customized to your organizational priorities and needs and designed to synchronize all existing policies or playbooks. Tabletop exercise with customized scenario, RANE proctor, and written after action report.	**Cyber Risk Monitoring & Analysis** Ongoing source of relevant intelligence on cyber threat landscape, technology, and vendors and the implications to your organization.
Executive/Board Reporting & Briefings Develop a framework for presenting to senior leadership, including briefing and presentation support.	**Forensic Evaluation & Remediation Team** On-demand incident response team to conduct forensics and remediate an incident at your site.	**Vendor Evaluation, Referral, & Response** Provider-agnostic sourcing and vetting of cybersecurity and information technology vendors to get you the best solution for your needs.

Update Information Security Policy, create supplemental policies (BYOD, travel, etc), assist in training workforce on policy.

Assess technical deployment team and existing incident response plan. Assist with synchronizing incident response playbooks/policies.

Perform tabletop exercise with all necessary players within organization.

Begin data identification, mapping, and compartmentalization exercise. Implement classification system and help select best data governance tool.

RANE CHECKLIST

Filling the Breach: Keys to Meeting SEC Cyber Requirements

Top company executives and board members still not certain what exactly they are required to do and reveal in the event of a breach now have new federal pronouncements to decipher — and learn to follow.

The 2018 SEC Cyber Disclosure Guidance, issued on February 26, continues the agency's emphasis on sound data protection practices while reminding us that preparation is critical — not just for the sake of operational continuity, but also to ensure your Board truly understands the impact of serious cyber events.

Of course, as with any government document, it isn't always easy to tease out the practical answer to one of the most critical questions facing enterprises these days: How do you prepare your organization's cybersecurity to ensure you will be ready to provide the right information in the event of a serious breach?

It is now necessary, for instance, to have immediate access to impact assessments of cyber events for both internal and potentially external release. SEC officials have encouraged utilizing the 8-K form (notification to investors of significant events) for significant cyber incidents.

RANE has previously provided basic cyber preparation recommendations (RANE, September 14, 2016, "SEC Cybersecurity Audits: Getting Ready for the Close-up"), but the latest agency guidance means companies need to up their game.

What follows are some basic practices recommended by RANE to ensure that your company, C-Suite and/or Board of Directors are prepared to meet their reporting requirements. They are divided into two categories: (1) SEC reporting requirements — preparing for potential internal and public reporting (2) Cyber Operational and Organizational Resilience — preparing a successful foundation for cyber incident response.

SEC Reporting Requirements:

1. There must be **continuous analysis** of the potential impact of cyber events on the company and specifically on the impact on resources of the company — operational, financial and organizational.

2. The company must have a clear process for **designating the severity of a cyber event** and determining whether it rises to the level to be reported to the SEC, other state regulators and potentially to investors.

3. The determination of whether an incident rises to the level of an 8-K report should be based on **reporting of operational interruptions and resulting effects**, initial estimates of monetary impacts, and where applicable, estimates of costs arising from forensic investigations and costs to ensure information systems can return to normal operation.

4. The metrics for a serious cyber incident should be **prepared in advance in a consistent format** approved by legal counsel, information security, communications specialists, senior management and the Board of Directors.

5. Your **Board of Directors** must be involved in the determination for reporting cyber incidents as required by the SEC.

6. Implement very specific data breach information collection policies **tailored to your company**. And don't look to the SEC for a specific procedure — its guidance is more general. You should immediately be collecting any relevant evidence or data available, such as audit logs and relevant captures of data.

7. Triage your data so that you will be able to pinpoint damage, disruption or loss of data. **Data Governance is critical** — if you don't know where (and what) personal or other data is held that may be subject to regulatory reporting requirements, you are already in the danger zone. Reporting will be more difficult and possibly erroneous unless you prepare reporting vehicles in advance.

Cyber operational and organizational resilience:

8. You must have clear, concise policies governing cybersecurity, breaches, and disclosure of incidents internally and externally all the way to the Board level. Informal "playbooks" or unwritten rules **will not suffice here**. Adopt best practices in these areas and ensure they are endorsed at all levels of the Company.

9. Synch up your lines of communication in the event of a serious cyber incident — this should be part of an **Incident Response Plan**. Understanding how information will flow up to the C-Suite and Board is mandatory.

10. **Board engagement** is critical even before an incident occurs. The SEC guidance requires disclosure by public companies of the involvement of their Directors in cyber risk management.

11. Your Board composition and organization should reflect the importance of cyber risk management. Many boards are adding cybersecurity committees and direct reports by their cyber experts (such as **Chief Information Security Officers** — CISOs)

12. Your Board must receive regular and formalized reporting on cybersecurity readiness and resilience. Be sure that you establish clear metrics regarding preparedness and incident response. A "dashboard" with different colors is **not sufficient**.

13. Be prepared to **call in the experts** if necessary. Establish a relationship with a good cyber forensic investigatory firm in advance so they "know" your networks when a crisis occurs.

14. **Practice, practice, practice** — and make sure your Board is included. Use an exercise or simulation to test the effectiveness of your response and communication. Make sure that you apply lessons learned to refining procedures and reporting.

RANE CASE STUDY

The Value of a Customized Approach to Incident Response and Resiliency

A client attended a RANE Cybersecurity Webinar that highlighted the importance of testing an incident response plan (IRP).

With companies facing new and more advanced cyber threats year after year, the panel of RANE experts recommended putting into place an annual tabletop exercise to regularly test a company's incident response plan. After attending the webinar, the client realized they were long overdue on testing their IRP and chose to leverage RANE's capabilities to get back on track. This would turn out to be very different from the typical tabletop exercise.

RANE tapped in-house subject matter expert and Executive Director of Cyber & Information, Rhea Siers, to lead a tabletop exercise and assess the effectiveness of the company's Incident Response Plan. The company was impressed by the unique and customized methodology used for this exercise.

RANE's Approach

One of the distinctive aspects of the exercise was the preparation put in beforehand. Siers conducted thorough research in order to become familiar with the company and how they present their strengths to investors and clients. This included highly specific information about the company's web interfaces, recently acquired companies, and their product offerings. In addition to research on the company, research was completed on relevant cyber threats and jurisdictions in which the company does business. The information gathered was used to customize the exercise and make it specific to the company, their compliance challenges, their industry, and its unique organizational dynamics.

The exercise participants included the company's entire Incident Response Team, representing multiple levels and areas of responsibilities. The group was given a set of realistic scenarios tailored to their specific roles — with actual references to the company's products, apps and portals targeted by a range of potential cyber threats. Some examples of these scenarios include hacks of the company's social media, disruption of its mobile apps, malware and ransomware attacks against the company's network, and Personally Identifiable Information (PII) being leaked to the Dark Web. During the exercise, participants logged the steps they took and discussed as a group their reasons for taking these steps. Rather than just facilitating the discussion, Siers was an active participant, allowing the other participants to share potential ideas and responses with her own recommendations and follow-up questions. The customization and attention to detail put in before, during, and after the exercise commanded the attention of the participants, and set RANE's approach apart from previous tabletop exercises they had experienced.

Key Takeaways

The group's ultimate goals were to figure out how to communicate the issues and the plan for resolution to their board of directors and C-Suite executives. From the exercise, they were able to identify where communication about an incident was especially important, both internally and externally. It allowed the team to realize what specific role each person had in each incident, even if they were not a part of the IT or cyber departments. This case demonstrates the value of a customized and interactive approach to a tabletop exercise:

- **An expert facilitator as an active part of the discussion** was one of the key differentiators of this exercise. Siers combined her operational and legal experience to provide a more holistic approach. Siers was selected as a Cyber Trail Blazer by the National Law Journal in recognition of her work in devising legal strategies for cyber vulnerabilities and incident response, and she served at the National Security Agency and in the US Intelligence Community for over thirty years, including as the Deputy Associate Director for Policy. Siers is frequently quoted in different media regarding cybersecurity, cybercrime, intelligence issues, and related law and policy. She used her expertise to advise and guide the group through the exercise, giving recommendations and feedback throughout.

- **The preparation put in beforehand** to design the exercise to meet the specific needs of the organization was another key differentiator. Siers conducted thorough research in order to become familiar with the company. The information gathered was used to personalize the scenarios and customize it to their specific company, its configurations, and its industry, in turn resulting in a more robust and realistic test of the Incident Response Plan.

- **Including members of several different roles and disciplines** was crucial to the success of the exercise, as any crisis requires multiple touch points and areas be involved in resolution of an incident. Siers made sure the tabletop included employees from communications, legal, compliance, and HR in addition to IT. Representation from multiple functional areas is essential to a successful IRP.

RANE

Risk Assistance Network + Exchange

www.ranenetwork.com | 1.844.786.RANE | info@ranenetwork.com