CYBERSECURITY

Incident Response Preparedness

Cybersecurity threats continue to expand both in numbers and sophistication. With each iteration, the risk of financial and reputational harm increases exponentially. Malicious actors run the gamut from traditional criminals to nation-state actors, political and social activists, business competitors, and disgruntled employees or clients. As cybercrime continues to evolve, the chances that you will be impacted increase as well. Even if you have a solid cybersecurity program in place, it is likely that eventually you will be the victim of a breach. The question then becomes, how will you respond to it?

THE Consortium Solution

Properly handling a likely attack on your systems requires developing an effective Cybersecurity Incident Response Team (CSIRT) capability. The expert cybersecurity professionals at Consortium Networks help you build an effective CSIRT that provides these key capabilities:

- A repeatable, measurable framework for responding to various cybersecurity incidents.
- Consistent triage, mitigation, and remediation.
- Executive and organizational awareness of cyber incidents in a business context through summarized analysis and regularly scheduled briefings.
- A format to document play-books/run-books that provide high-level operational tasks for incident response.
- Meaningful key performance indicators (KPIs) and metrics to ensure ongoing health and demonstrated success of the program.
- An ongoing communication loop between the CSIRT and key business stakeholders that continuously refines the process through post-incident review (PIR) and simulated tabletop exercises.

The Consortium CSIRT program provides you with an expert evaluation of your current incident response (IR) capabilities to identify strengths and areas for improvement, and to provide practical recommendations and supporting documentation for development and formalization of your CSIRT program.

DEVELOPING THE
Incident Response Plan (IRP)

Consortium's IRP development process involves:

- Interviews with key individuals in your organization to identify existing CSIRT members or individuals who de facto perform in that role, as well as business constituents, to understand the current IR program maturity.
- Evaluating the architectural and technical design of the CSIRT program infrastructure (decision alerting, incident tracking, evidence collection).
- Reviewing the documented and ad-hoc processes that form the foundation of the existing CSIRT capabilities.
- Assessing the communication processes between the CSIRT and existing constituents who are decision makers or who require situational awareness.

Once the IRP development process is complete, Consortium will provide documentation for an incident response framework customized to your business. The framework will be accompanied by recommendations for tooling and staffing resources that will further enhance the program. The framework will initially focus on developing response activities for information security, information technology, and senior business executives with the capability to expand to support the addition of response activity playbooks for other business partners such as marketing/PR, legal, privacy, third party services providers and others. The IRP development engagement concludes with a presentation summarizing the results and providing guidance on next steps.

LEARN MORE: CONSORTIUM.NET/CYBERSECURITY-INCIDENT-RESPONSE-PREPAREDNESS/

ABOUT
Consortium Networks

Consortium Networks is the trusted Cyber Concierge that helps our clients solve their toughest cybersecurity challenges. We are a cybersecurity risk, technology, and networking organization on a joint mission to connect and educate the community. We founded Consortium to change the "game" and help our clients make sense of the spaghetti labyrinth they call cybersecurity. By mapping our clients' controls to industry standards and risk, we help them reduce complexity and risk to their organization and people. The outcome: clients will quickly understand their gaps and realize the impacts of their investment decisions, strengthening their cyber hygiene, and ultimately, protecting the business.

Our Concierge way of working sets us apart and follows four timeless principles of customer service: attitude, consistency, service, and teamwork. We are devoted to helping others selflessly in both our work and personal communities. For more information, visit consortium.net.