CRA Charles River Associates

Cybersecurity Pre-Incident Services for Proactive Threat Detection and Cyber Hygiene

Increase visibility, mitigate risk, manage threats

AT A GLANCE:

CRA's Pre-Incident Services to Clients

- Incident readiness and resilience assessments
- Intelligence based penetration testing, adversary simulation, red and purple team assessments
- Incident response and crisis communication strategy
- Forensic and logging readiness
- Tabletop exercise and first responder training
- Privacy impact assessments
- HIPAA, NIST CSF, ISO risk assessments
- Insider threat and threat modeling

"Organizations struggle to balance cybersecurity with the need to run the business. Chief information security officers (CISOs) can help by developing processes that enable risk-based decisions while protecting against security threats and prevent data breaches and other cybersecurity events."

—Gartner, 2020

Cybersecurity issues we address

One of the key issues organizations are facing today is the ability to accurately and efficiently obtain information from the IT estate in order to understand cybersecurity risks, make informed decisions, and take appropriate actions. CRA addresses the fundamental problem of poor cybersecurity hygiene by analyzing organizations' two areas – Incident Readiness program, and Security hygiene & Vulnerability management' – to help clients with the ability to detect unmanaged IT assets and identify key baseline security controls, to further streamline the security transformation.

Proactive services tailored to all industry sectors

CRA has developed a cyber solution tailored to multiple industry sectors such as Healthcare, FI, manufacturing and retail. Our solution combines the inter-dependent areas of IT asset management, incident and threat managements, enterprise risk and crown jewels identification.

Deep IT and cyber forensics skills

CRA offers unmatched expertise in cyber threat detection and response, attack surface exposure and reduction, and sensitive data identification – and helps clients maintain robust cyber hygiene and compliance with ISO 27001 and NIST Cybersecurity Framework (CSF).

Incident response retainer service

CRA utilizes the same underlying network and endpoint technology infrastructure, allowing seamless expansion of the service into cyber investigations.

30%
of breaches involved a trusted employee
(Verizon DBIR 2020)

22%
of folders on the network were available to every employee
(Varonis)

69%
of organizations believe conventional security measures to be ineffective
(Ponemon Institute's Cost of Data Breach Study)

68%
of business leaders feel their cybersecurity risks are increasing
(Accenture)

Lessons learned
- Data and tools to effect strategic and continuous improvement

Recover
- Demonstrate the ability to recover quickly and efficiently

Respond
- Incident Response (IR) retainer for ongoing support
- Implement defensive measures

Identify
- Improve system visibility
- Incident management plans
- Vulnerability intelligence

Protect
- Elevated access controls
- Data protections

Detect
- Vulnerabilities and patches
- Sensitive data
- Detect and hunt threats
- Risk assessment

Why CRA?

- Operating from nine countries around the world, CRA's clients include 83% of the Fortune 100 companies and 94% of the AmLaw 100 law firms
- Benefit of extensive experience in planning, building, and operationalizing a threat management and privacy program across multiple jurisdictions
- Certified under ISO 27001 security and data privacy requirements
- Industry leading incident response provider

CRA's Forensic Services

CRA's Forensic Services Practice was recently honored in the National Law Journal's "Best of 2020" for being one of the top three Forensic Accounting Providers in the country, and by Global Investigations Review as one of ten forensic practices from around the world for handling sophisticated investigations. The Practice – including our state-of-the art digital forensics, eDiscovery and cyber incident response labs – has been certified under International Organization for Standardization (ISO) 27001:2013 requirements as part of our industry-leading commitment to our clients and their information security.

Illustrative example: The Panama Papers

The infamous Panama Papers Incident offer an illustration of what can go wrong from an IT and cyber perspective, and what could have been done to avoid, prevent and mitigate the damage.

Panama papers summary

11.5 million leaked encrypted confidential documents exposed the network of more than 214,000 tax havens involving people and entities from 200 different nations

How CRA could have helped
- Hygiene checks would have shown outdated, vulnerable systems
- Incident Readiness would have helped with effective communication strategy
- Adversary simulation would have identified the attack surface
- Help train the IT and Security staff on incident handling
- Developing ongoing security strategy

What went wrong?
- Unpatched systems, systems lacking encryption, insecure network design
- Poor cybersecurity hygiene
- Lack of effective security controls

Contact

Aniket Bhardwaj, GREM, GCIA, GNFA, GCFA
Vice President, Cyber Threat Detection & Response
+1-416-323-5574 | abhardwaj@crai.com

CRA Charles River Associates