CRA Charles River Associates

SOLUTION BRIEF

Cyber Solution for Law Firms

Increase visibility, mitigate risk, manage threats

AT A GLANCE:

CRA's Services to Law Firms

- Inventory of hardware and software assets
- Monthly health checks
- ePII/sensitive data reports
- Prioritized vulnerability and patch report
- Security strategy road map

> "Lawyers must assess the risks involved in the use of electronic devices and systems that contain, or access, confidential client information and to take reasonable precautions to ensure that that information remains secure."
>
> —California State Bar Committee on Professional Responsibility and Conduct

Law firms are custodians of very sensitive information

Due to the nature of their business, law firms possess a tremendous volume of valuable documents and data, which are extremely attractive to hackers of a variety of motivations. Successful cyber-attacks can cause a severe negative impact to a law firm's operations and catastrophic damage to a law firm's reputation.

A cyber solution tailored to law firms

CRA has developed a cyber solution tailored to the needs of law firms. Our solution combines the inter-dependent areas of IT asset management, security, risk and sensitive data.

CRA offers 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%

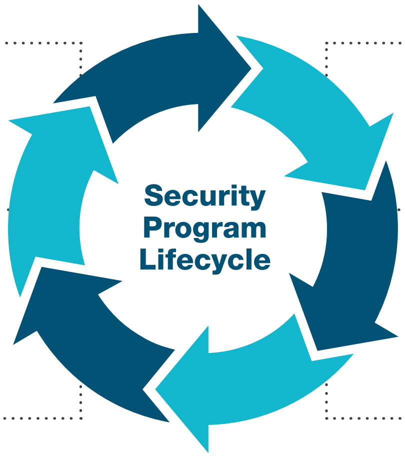
of organizations believe conventional security measures to be ineffective

(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

- Health checks would have shown outdated, vulnerable systems
- Suspicious findings would trigger a CRA threat hunt
- Seamless integration from assessment to an IR investigation Immediate remediation

What went wrong?

Unpatched systems, systems lacking encryption, insecure network design

Contact

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

CRA Charles River Associates