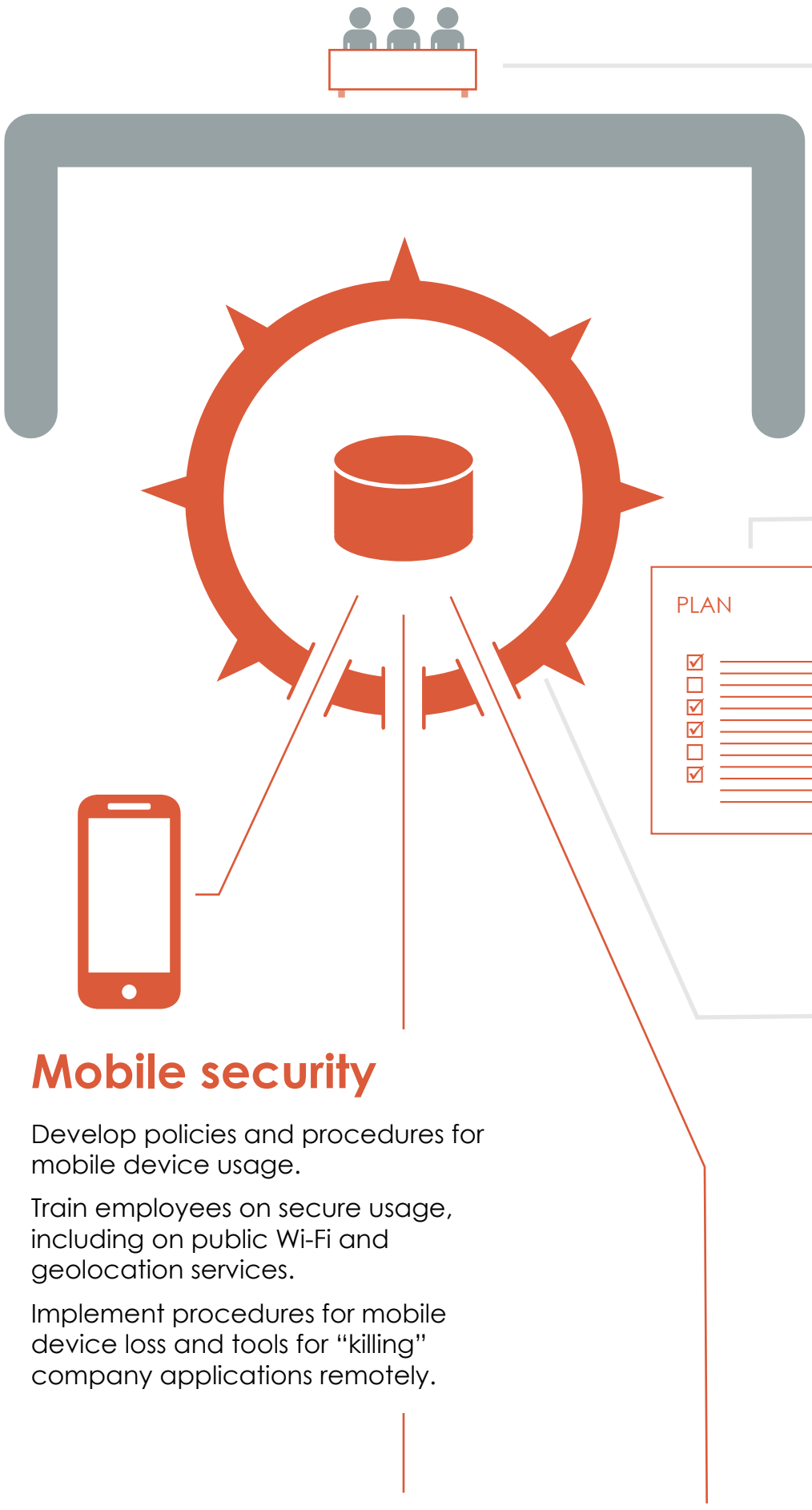
Kramer Levin

Cybersecurity:
SEC guidance on best practices

At the end of January, the U.S. Securities and Exchange's Office of Compliance Inspections and Examinations (OCIE) released its "Observations on Cybersecurity and Resiliency Practices". Companies that employ or adapt these best practices — many of which are highlighted below — will likely better weather a cyber-storm.



Governance

Actively involve C-suite in setting the strategy of cybersecurity and resilience programs.

Regularly brief and consult the board on the strategy.

Develop and conduct an assessment of relevant cyber risks.

Write and test comprehensive cybersecurity policies and procedures.

Incidence response

Develop an incident response plan (IRP).

Develop a business continuity plan.

Develop a breach communication plan (BCP).

Test the IRP and BCP through "table top" exercises.

Ensure core business systems are resilient, geographically dispersed, and stress-tested.

Data loss prevention

Utilize vulnerability scanning tools, perimeter security, threat-identification software, and similar tools.

Maintain system logs and inventories of hardware and software.

Conduct insider threat monitoring.

Secure and decommission retired hardware and software.

Regularly train employees on policies and procedures, vulnerabilities, and breach identification.

Mobile security

Develop policies and procedures for mobile device usage.

Train employees on secure usage, including on public Wi-Fi and geolocation services.

Implement procedures for mobile device loss and tools for "killing" company applications remotely.

Vendor management

Conduct due diligence on third-party providers with access to protected data.

Use vendor management programs to enforce security requirements and terminate vendors if necessary.

Review contract terms with vendors concerning data responsibilities, liability, and reporting.

Access controls

Develop a data map, and impose clear policies to restrict data access to authorized users.

Require the use of strong, frequently-changed passwords.

Revoke system access for former employees and vendors.

Monitor failed login attempts and account lockouts.

For more information, contact

Samantha V. Ettari settari@kramerlevin.com
Alan R. Friedman afriedman@kramerlevin.com
Daniel Lennard dlennard@kramerlevin.com