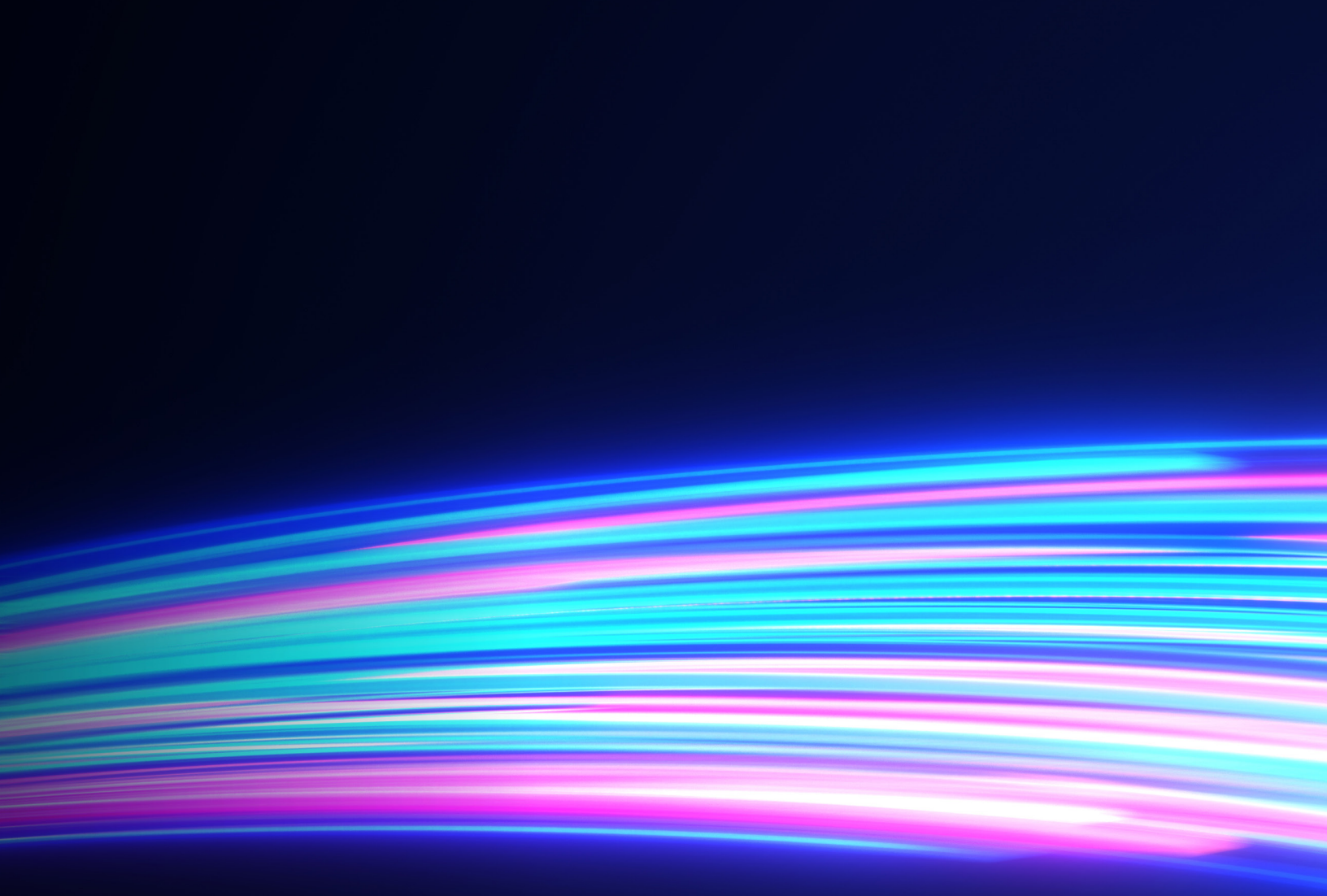


INCIDENT RESPONSE SERVICES

ATTORNEY ADVERTISING

Ballard Spahr LLP

Incident Response Services

Our team of attorneys across the country puts clients and their specific needs first. We go beyond templates, leveraging the lessons we have learned over years as members of our cross-disciplinary Privacy and Data Security Group—conducting compliance and transactional services, leading investigations and litigation, and responding to hundreds of incidents across the globe.

PRE-INCIDENT PREPAREDNESS

Careful planning is the best way to ensure an efficient and defensible response to an incident. Key components of our proactive approach include:

- Privileged and periodic cybersecurity assessments
- The creation and refinement of data security and cyber incident response plans, including incorporating non-information security personnel to comply with legal, regulatory, and public filing requirements
- Employee/vendor training to implement a holistic information security program
- Exercises involving simulated cyber incident scenarios
- Periodic updates on the evolving threat landscape
- "Lessons learned" reviews from cyber incidents around the globe

We develop company-specific programs that provide workable response solutions before they are needed and better position clients to defend their interests after an incident.

INCIDENT RESPONSE

We are available around the clock, every day, to quickly mobilize a scalable response to any cyber incident.

We have handled hundreds of incidents in a variety of areas—with a significant concentration in the financial services, media and entertainment, health care, hospitality, insurance, manufacturing, technology, and education industries. We handle incidents from garden-variety data breaches to national security threats, seamlessly integrating into our clients' internal and external teams to craft a comprehensive and tailored response under the protection of attorney-client and other applicable privileges. We assist in:

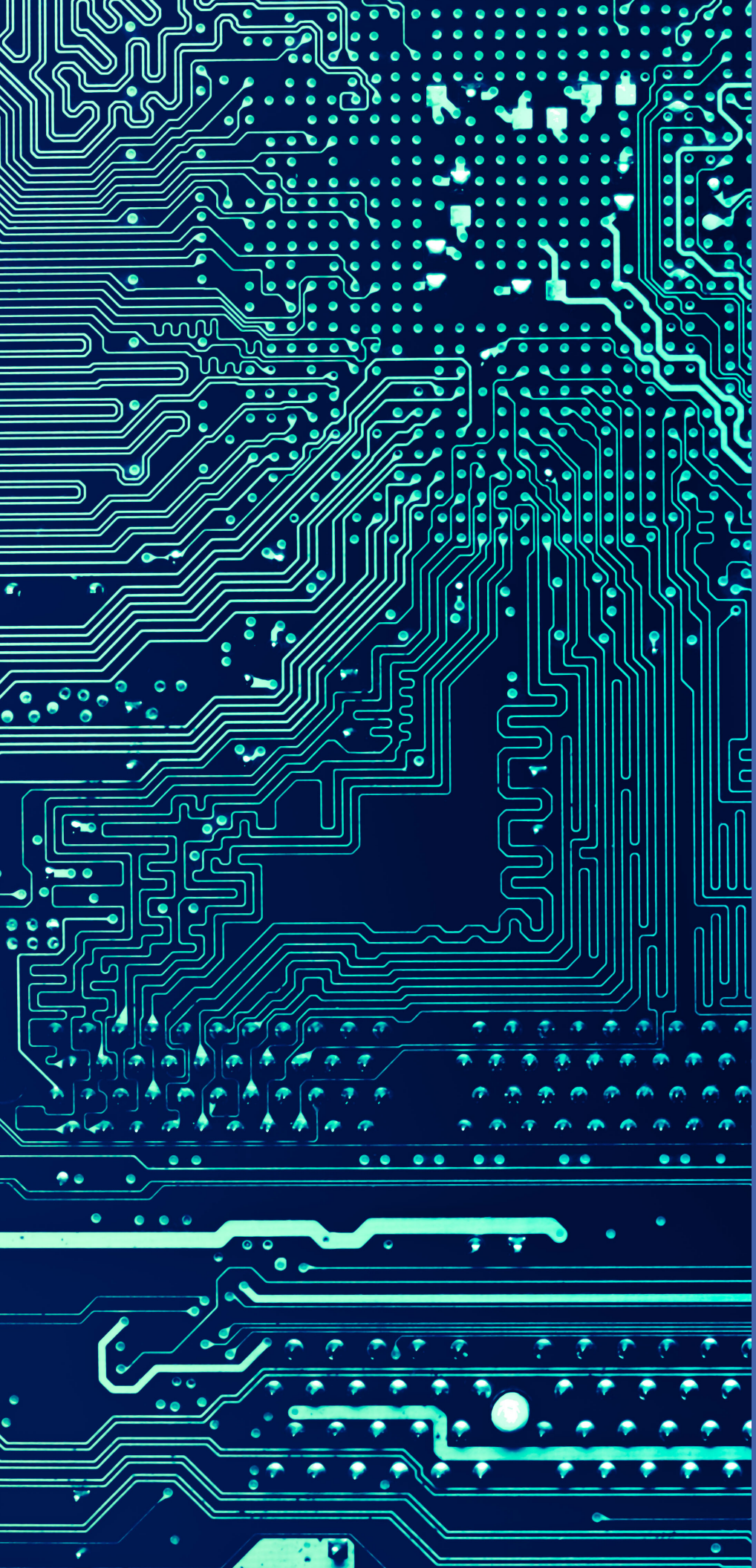
- Directing investigations and responses to cyber incidents
- Interacting with law enforcement and intelligence communities, as well as privacy and cybersecurity regulators at the federal, state, and international levels
- Devising strategies and preparing materials for cyber incident notifications
- Implementing post-incident remediation plans

We help clients prepare for and manage all contingencies that may follow such notifications and the public release of information about cyber incidents.

INVESTIGATIONS AND LITIGATION

Our team members have engaged in hundreds of internal investigations covering every major type of cyber incident, including network intrusions, identity and intellectual property theft, ransomware, and internet-facilitated fraud. We also have significant experience in responding to non-malicious cyber incidents, such as the lost device, operational error, inadvertent electronic transmission, or technological glitches that result in data exposure.

We handle pre-litigation planning and negotiation, eDiscovery and pre-trial litigation, as well as trial and appellate advocacy on a full range of privacy-related disputes. We have experience in privacy class action litigation across various industries, including financial services, insurance, life sciences, education, health care, communications, and technology.



CONTACTS

GREG SZEWCZYK
Practice Leader, Privacy and Data Security
szewczykg@ballardspahr.com
303.299.7382