Cybersecurity Best Practices from CISA and Critical Infrastructure Sectors

April 1, 2022

Robert Kang
Ruben Arredondo
Romaine Marshall

Always exceed expectations through teamwork and excellent client service.

2021 and 2022 ACC CLO Survey Results

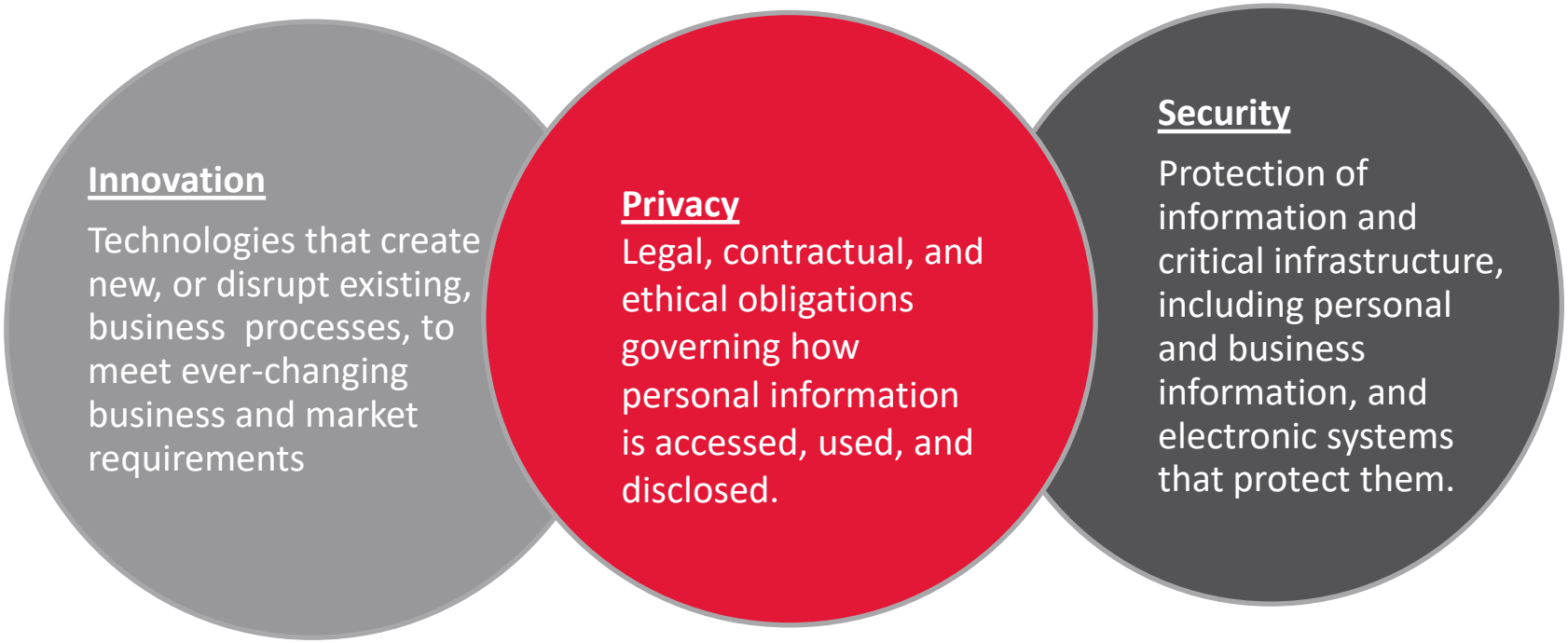
KEY FINDINGS

THE LEGAL DEPARTMENT'S VALUE TO THE BUSINESS

CYBERSECURITY, COMPLIANCE, AND DATA PRIVACY ARE THE MOST IMPORTANT ISSUE AREAS FOR BUSINESSES

For the third consecutive year, cybersecurity, compliance, and data privacy top the list as the most important issue area for businesses rated by CLOs. However, this year for the first time, cybersecurity has overtaken compliance for the number one spot.

Data means …



Altogether, a patchwork of legal, regulatory, and industry standards is fast-emerging

Start with Cybersecurity …

"Cybersecurity is the mother of all problems. If you don't solve it, all the other technology stuff just doesn't happen."

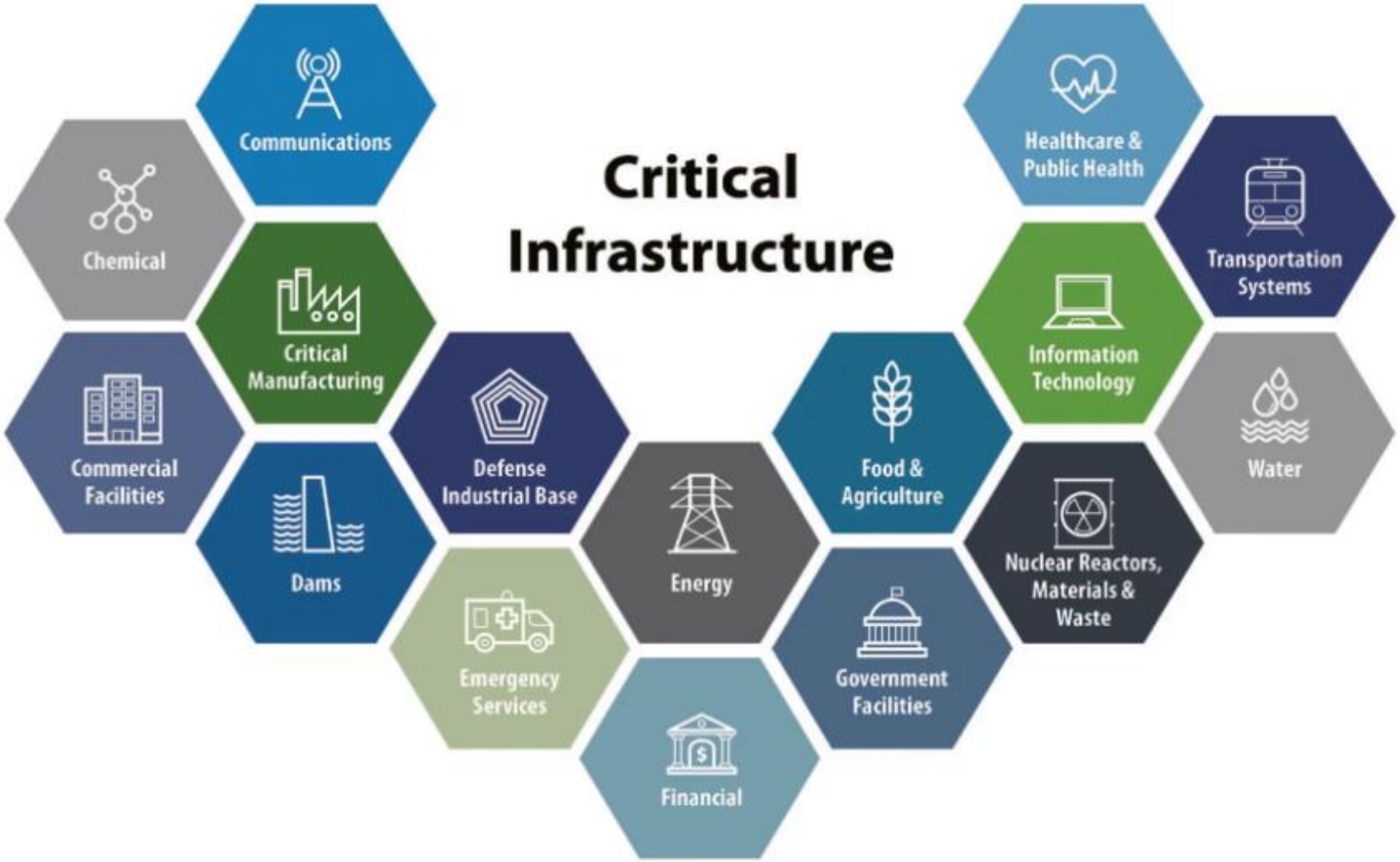
- Charlie Bell, Microsoft Chief of Security

Source: https://www.wsj.com/articles/microsofts-new-security-chief-says-it-is-time-to-take-shelter-in-the-cloud

- Since 2018, “leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.”
- ”[C] reated to work across public and private sectors, challenging traditional ways of doing business by engaging with government, industry, academic, and international partners.”
- Vision: a secure and resilient critical infrastructure for the American people.

Critical Infrastructure

- Presidential Policy Directive 2021
  - “Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.”



© US Cybersecurity & Infrastructure Security Agency (CISA)

The Threats

Digital Transformation, the Pandemic, Russia …

- *"Digital transformation is the process of using digital technologies to create new, or even disrupt the current business processes, the culture, customer experience, to meet those ever-changing business and market requirements."*

- *"We've seen two years' worth of [DT] in two months."* - Satya Nadella (Microsoft CEO, April 2020)."

- *"There is now evolving intelligence that Russia may be exploring options for potential cyberattacks." Pres. Biden Fact Sheet (March 21, 2022)*

National Security

Accelerated by DT, the Pandemic, and now, Russia. What next?

Where were you 9/11, 2001?

Laws, Regs, Industry Standards

A Blooming Cybersecurity Patchwork

- "At least 38 states, Washington, D.C., and Puerto Rico introduced or considered more than 280 bills or resolutions that deal significantly with cybersecurity."

- At least 20 states enacted 46 key cybersecurity-related bills in 2020

- Federal Trade Commission:
  - "*What are the Industry Standards? Are We Meeting Them?*"
  - "Cybersecurity is not an IT issue but a board issue."

- Securities and Exchange Commission:
  - "[S]tay abreast of [technological] developments … be ready to bring cases involving issues such as crypto, cyber, and fintech."

Executive Order – May 12, 2021

- Improving the Nation's Cybersecurity
  - "To understand your risk, *immediately convene their leadership teams to discuss the ransomware threat and review the corporate security posture* and business continuity plans to ensure you have the ability to continue or quickly restore operations.
- Implement "high impact" best practices:
  - MFA, ED & R, encryption
  - Support security team-approach
  - Patch management

Cyber Incident Reporting for Critical Infrastructure Act – March 17, 2022

- 24 hours to:
  - *A covered entity that makes a ransom payment as the result of a ransomware attack against the covered entity shall report the payment to the Agency not later than 24 hours after the ransom payment has been made.*
- 72 hours to:
  - *A covered entity that experiences a covered cyber incident shall report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber incident has occurred.*

Biden Fact Sheet – March 21, 2022

- Act Now to Protect Against Potential Cyberattacks
  - *"There is now evolving intelligence that Russia may be exploring options for potential cyberattacks."*
  - Urges companies to execute eight broad steps with urgency, including:
    - Educate employees to common tactics of attackers
    - Run exercises and drill your emergency plans so that you are prepared to respond quickly to minimize the impact of any attack;

1. Law Enforcement (FBI)

Operates under the jurisdiction of the Department of Justice (DoJ)

Is the domestic intelligence service and federal law enforcement agency of the United States

- Investigates terrorism, counterintelligence, public corruption, civil rights violations, cyber crimes, organized crime, white collar crime, violent crime, and weapons of mass destruction threats[2]

Mission: "To protect the American people and uphold the Constitution of the United States."[3]

1. Law Enforcement (FBI)

Methods of Combating Cyber Threats

- Investigate Crimes
  - "investigate computer intrusions, theft of intellectual property and personal information, child pornography and exploitation, and online fraud"
- Cyber Action Team (CAT)
  - Rapid response team of cyber experts used to quickly determine a hacker's signature and the extent of the breach

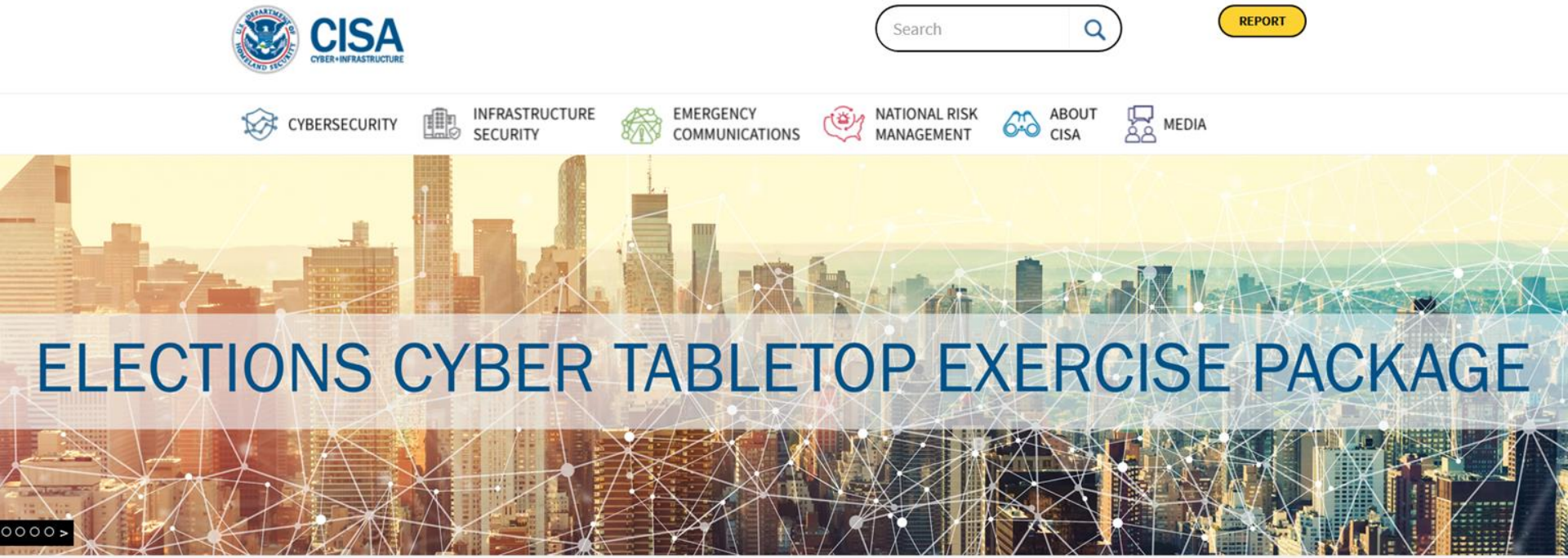
1. Law Enforcement (FBI)

Operates under the jurisdiction of the Department of Justice (DoJ)

Law Enforcement investigates crimes and prosecutes malicious actors

Mission: "To protect the American people and uphold the Constitution of the United States."[3]

2. Infrastructure Protection (DHS)



2. Infrastructure Protection (DHS)

Mission: “The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards.”

DHS has five core missions:

- Prevent terrorism and enhancing security
- Secure and manage our borders
- Enforce and administer our immigration laws
- Safeguard and secure cyberspace
- Ensure resilience to disasters

Created in response to the September 11 terrorist attacks

2. Infrastructure Protection (DHS)

Mission: "The vision of homeland security is to ensure a homeland that is safe, secure, and resilient against terrorism and other hazards."[15]

DHS Protects Stuff

Created in response to the September 11 terrorist attacks

Protections / Responses

Making a CISA Cost-Benefit Assessment

Measure Your Return on Investment / Common CISA Services & Considerations

- Physical Security & Cybersecurity Assessment
  - Are you ready to act on CISA recommendations?
  - These may be discoverable

- Information Sharing - CISA 2015 & More
  - Information shared with USG may be subject to FOIA.
  - Are you familiar with FOIA exemptions, including “PCII”?
  - Some services cost nothing. Others will require internal investment of time, resources & money. What services do you need?
  - Information Sharing - CISA 2015 & More

- Incident Response Flyaway Teams
  - Are you ready to sign CISA service agreements?
  - Are you ready to provide CISA with information about your systems?
  - Will you need to provide CISA access to your systems?
  - FOIA concerns return

Critical Energy/Electric Infrastructure Information (CEII) Defined

CEII is specific engineering, vulnerability, or detailed design information about proposed or existing critical infrastructure (physical or virtual) that:

1) Relates details about the production, generation, transmission, or distribution of energy;
2) Could be useful to a person planning an attack on critical infrastructure;
3) Is exempt from mandatory disclosure under FOIA; and
4) Gives strategic information beyond the location of the critical infrastructure.

See generally Section 215A(d) of the Federal Power Act, and Federal Energy Regulatory Commission (FERC) Order Nos. 833, 702, 630, 630-A, 643, 649, and 683 here

Critical Energy/Electric Infrastructure Information (CEII) Defined

CEII means a system or asset of the bulk-power system, (physical or virtual) the incapacity or destruction of which would negatively affect:

- National security
- Economic security
- Public safety or health, or
- Any combination of such matters

Source: see generally Section 215A(d) of the Federal Power Act, and Federal Energy Regulatory Commission (FERC) Order Nos. 833, 702, 630, 630-A, 643, 649, and 683 here

“Common Threads” Emerge

- Thousands of incidents and hours helping clients have revealed certain PROTECTIONS and RESPONSES
- Cybersecurity
  - Incident Response Plans (IRPs)
  - Risk Assessments (RAs)
  - Written Information Security Programs (WISPs)
  - Executive oversight (regular, meaningful updates)
  - Employee training and vendor management (TTX)

Incident Response Plans (IRPs)

- Why it's necessary
  - FTC: a reasonable plan, reasonably followed, may be the difference for a regulatory action.
  - SEC: recent enforcement actions have analyzed IRPs.
  - Federal Reserve/OCC/FDIC: 36-hour rule.
  - Insurance: an IRP is becoming mandatory by underwriters.
  - Reputational harm: consumers and other third parties increasingly intolerant of a botched response.
  - Business continuity: responding as important to survival than defending.

Risk Assessments

- What it is
  - an assessment of the potential technical, administrative and physical risks and vulnerabilities to the confidentiality, integrity and availability of personal or confidential information and systems.
- What it does
  - leads to policies, then standards, then procedures, all of which together serve to comprehensively outline objectives and administrative, technical, and physical controls.

Written Information Security Programs

- What it is
  - The policies and procedures that an organization maintains for *administrative, technical, and physical safeguards* to protect the privacy and security of personal information.
- What they do
  - In some states, WISPs are a 'Safe Harbor'
  - In some states, WISPs are required as an "industry standard"
  - Organizations generally required to
    - "evaluate and adjust the [Written] Information Security Program *in light of any changes to [your] operations or business arrangements* ….," i.e., emerging technologies, new threats.

NERC CIP: One of Several Cybersecurity Frameworks

"The secret to winning the innovation game lies in understanding what causes customers to make choices that help them achieve progress on something they are struggling with in their lives …. What job would consumers want to hire a product to do?"

Like other cybersecurity frameworks (NIST, CIS, ISO, SANS), CIP protections have 5 main jobs: *Identify, Protect, Detect, Respond, Recover.*

Violations occur when companies ignore the jobs to be done and build compliance silos leading to gaps, duplication, and even discrepancies between cybersecurity frameworks and implementation.

Identify the job to be done and then align frameworks, outputs, evidence gathering, etc.

*** From "Competing Against Luck" by Clayton M. Christensen. See generally Harvard Business School's "Working Knowledge" write-up on jobs theory**

Board, C-Suite, Legal Roles

When considering whether credit for a compliance program is appropriate in determining a civil penalty, the Federal Regulatory Energy Commission will look at the role of senior management/legal in fostering compliance:

- Education and proper oversight at Board level, C-suite
- Compliance programs should have an easily identifiable "beeline" between "boots on the ground"
- Generally speaking, in-house leaves all CIP concerns to IT/CIP SMEs or outside counsel when violations occur. Ethical?
- Writing is on the wall: Increased liability for fiduciaries for breaches of cybersecurity

For CEII

- Understand role of various cybersecurity frameworks, especially CIP; holistic implementation
  - *Framework for Improving Critical Infrastructure Cybersecurity* and related news, information: www.nist.gov/cyberframework
- Use FERC Lessons Learned to focus "boots on the ground"
  - *FERC Staff Report Details Lessons Learned from CIP Reliability Audits,* FERC (October 2021); includes 2017-2020 Lessons Learned
- Expose in-house legal to CIP work; use SMEs to train/mentor
  - Purpose is not to make in-house legal "experts" but to become proficient in the language of CIP/cybersecurity; spot potential risks; catch serious issues; involve Board and senior management.

CISA resources

- https://www.cisa.gov/shields-up
  - Latest Updates
  - Guidance for All Orgs.
  - Recommendations for Corporate Leaders and CEOs
  - Ransomware Response
  - Steps You Can Take to Protect Yourself
  - Additional Resources

About Armstrong Teasdale

Overview of Armstrong Teasdale – Firm Information

For 120 years, Armstrong Teasdale has forged long-term relationships with clients large and small around the globe.

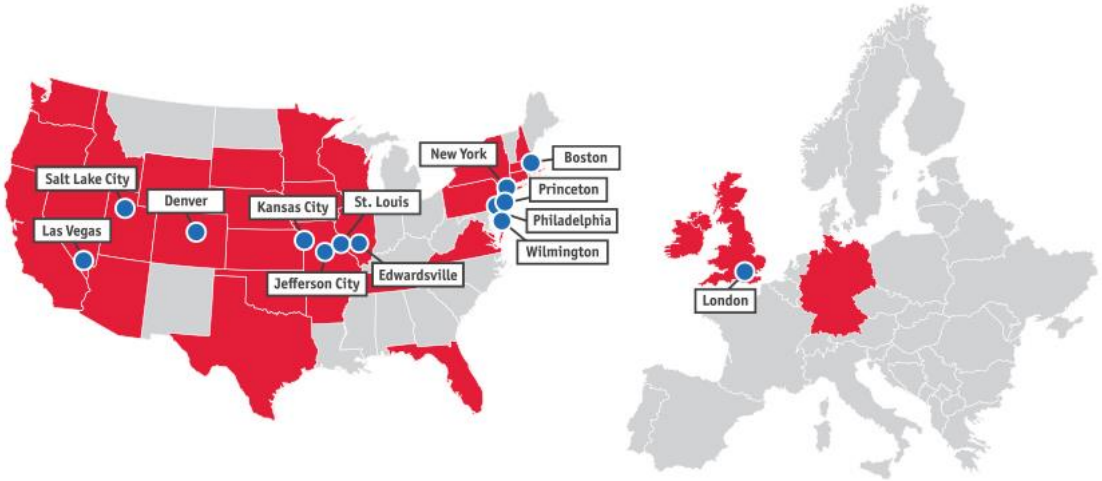
360+
— LAWYERS —

300+
— STAFF —

— SERVING OVER —
125+
FORTUNE 500 COMPANIES

— AM LAW —
200

With 13 offices across the U.S. and in London, our lawyers are licensed to practice in 30 states plus Washington, D.C., as well as in the U.K., Germany and Ireland.



**As of Dec. 2021*