The Evolving and Chaotic Environment of Consumer Data Privacy Regulation

What regulators expect and the pressure on timing and adoption for existing businesses.

Scott Madsen

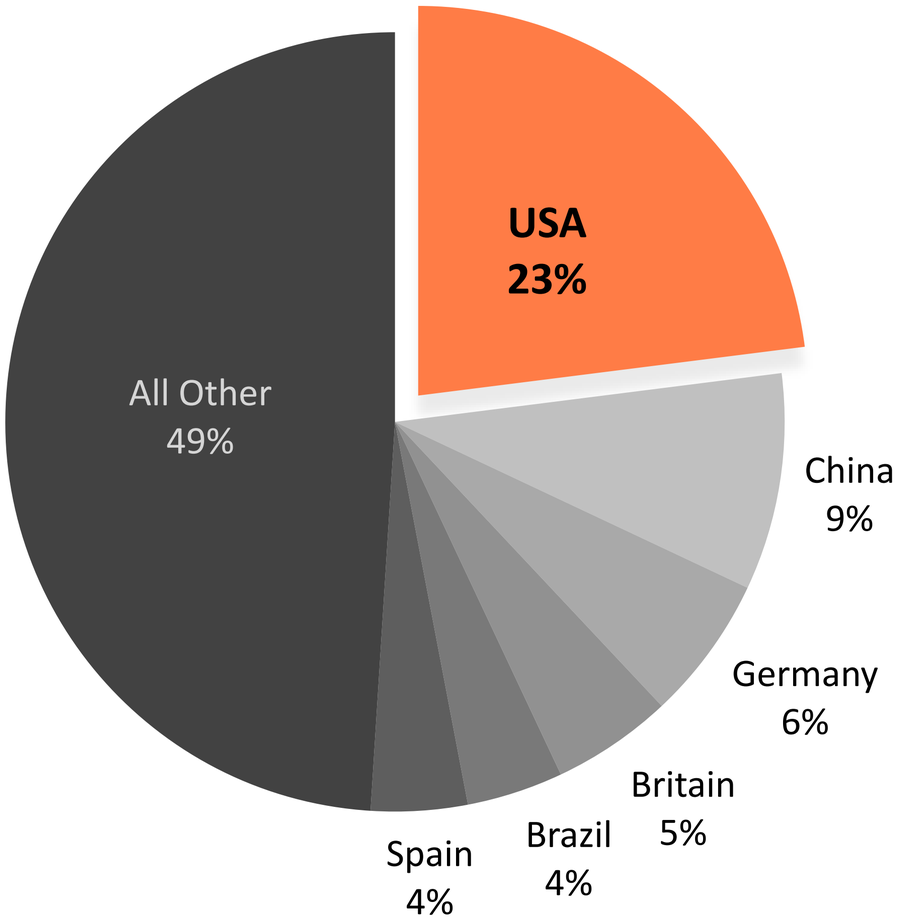
Landscape of threats & regulating data privacy.

The right team will consist of the following:

1. Privacy Attorney — I tell all the clients I work with that in-house council is great but at the end of the day, you really need someone who lives in this space. A good privacy firm will not only help you navigate this space but will also be an integral part of the team to make sure you understand all of the pitfalls; because there are a lot of them.
2. Cyber Security Firm — Internal IT does their best but you need an IT that fully understands what regulations are required and how to implement the security stake to ensure it is acutely compliant.
3. External Auditors — Regardless of the niche you service in Financial Services, you will have an auditor come check once a year. Not only to prepare for your regulatory audits, but to verify that the privacy attorney and security firm have implemented the correct controls.

- With all 3 of these firmly in place now you're ready to complete and formalize your SOP's to be in compliance.
- At least once a year, run an internal audit making sure that all of these boxes have been checked.

Highest target of cyber crime.



United States represents 23% of the worlds cyber crime focus.

Source: www.enigmasoftware.com/top-20-countries-the-most-cybercrime

Highest targeted industries in the US

Over the past 6 years, offenders have focused on 5 main industries:

Source: netdiligence.com/cyber-claims-studies

- Professional Services
- Manufacturing
- Retail
- Financial Services
- Healthcare

Largest cyber-crime of personal data happens abroad.

- Russia
- China
- Brazil
- Nigeria
- North Korea

  Targets small to mid-sized banks in developing countries

Not Listed

Why are cyber criminals from these countries trying to penetrate your industry?

- Cyber crime out performs the drug cartels.
- Cyber liability will pay out more than disaster recovery policies by 2024.
- Quick cash grab.

Sources: secureblitz.com/top-countries-notable-for-cyber-criminals
https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

What is happening at the federal level?

Federal Agencies Jurisdiction — Criminal focused

The FBI oversees the following:

- Protects the U.S. against foreign intelligence, espionage, and cyber operations.
- Protects the U.S. against cyber based attacks and high-level technology crimes.
- Combat significant cybercriminal activity.

What about at the state level?

State Agencies Jurisdiction — Prevention focused

State agencies and prevention efforts vary per state. States looking to enforce against businesses:

- California (CPRA)
  Active state agency random audits and penalties enforced.
- Washington State (Policies in State Houses)
  TBD
- Oregon (Policies in State Houses)
  TBD
- Utah & Colorado
  Policies being enacted now for active enforcement.

What does this mean for the general market?

According to current state efforts, responsibility will fall directly on the shoulders of businesses and providers to police client privacy.

Under the CPRA, fines will be levied for each datapoint of personal data exposed.

- First Name
- Last Name
- DOB
- Address
- Etc.

Businesses would have to meet structured privacy policy criteria based on external state policy.

What does this mean for your company?

1. When you are out of compliance, not only do you have to pay the criminal, but now you have to pay the state if you were not following their regulation on data protection.
2. What state affects you? Any state you have clients in and meet the criteria for the regulation.
3. What does “out of compliance” mean? Depends on the state.
4. How often is regulation changing? Monthly to Quarterly
5. What can you be fined? Depends on the state and some don’t have a cap.

Burden on organizations

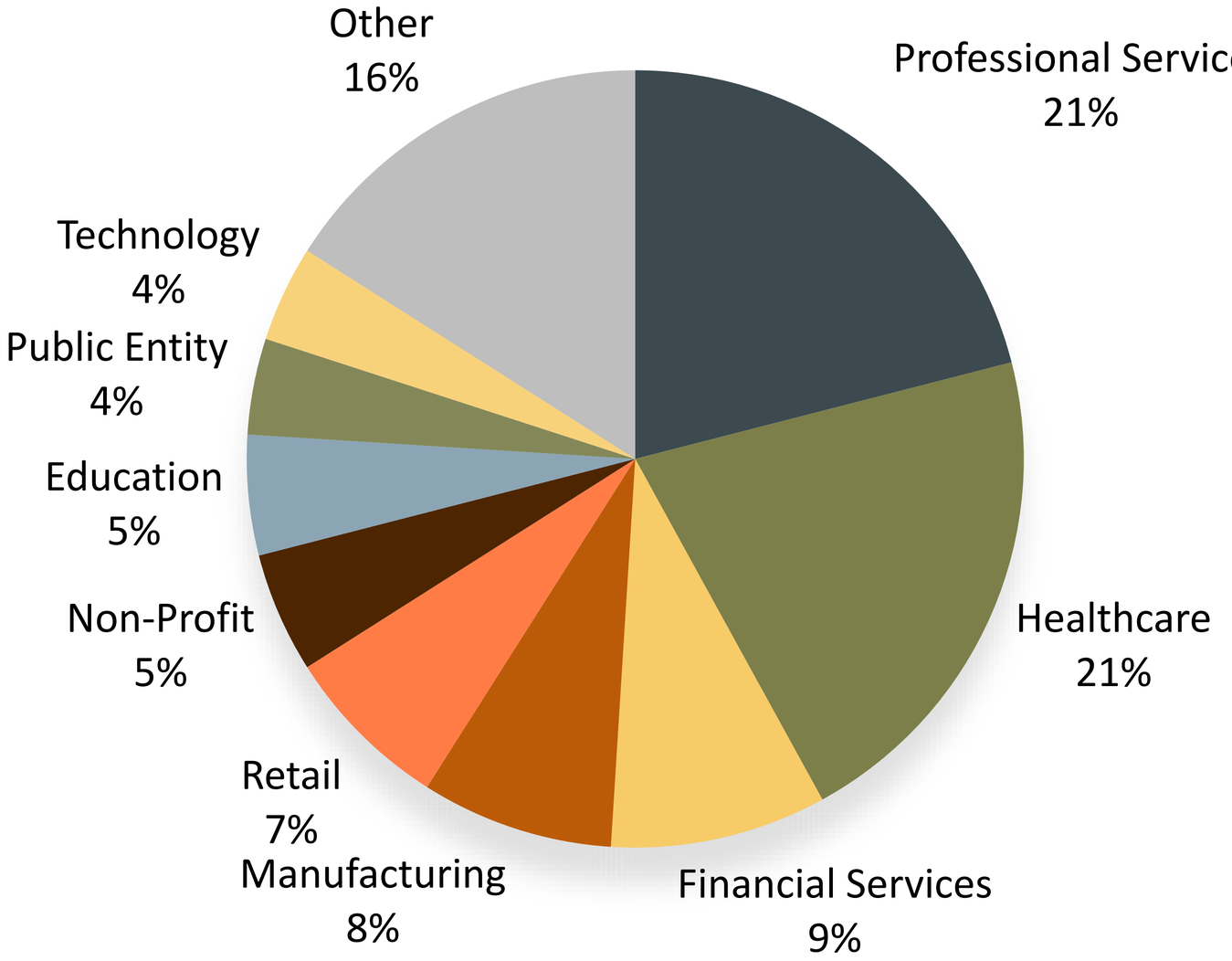
Operations:

- Privacy Policy
- Terms of Service
- Update SOP’s
  - Document internal audits of SOP adherence
  - Document employee error whenever it happens on a per instance basis

Technology:

- IT Department needs CE
  - Cyber threats are an evolving problem
  - As new threats emerge, IT staff needs to be trained & made accountable.
- All IT vendors have to provide SOC2 type 2 audits annually
- SOC2 packet needs to be prepared to be provided to auditors
  - Heavy documentation for internal trainings
  - Documentation for failed and updated processes
  - Disciplinary action and training for employees

Percentage of Insurance Claims by Sector



Source: netdiligence.com/cyber-claims-studies

In 2018, large companies (avg. $11B) made up for the majority of targets.

While in 2020, small to mid-sized businesses (avg. $84M) accounted for 99% of targets.

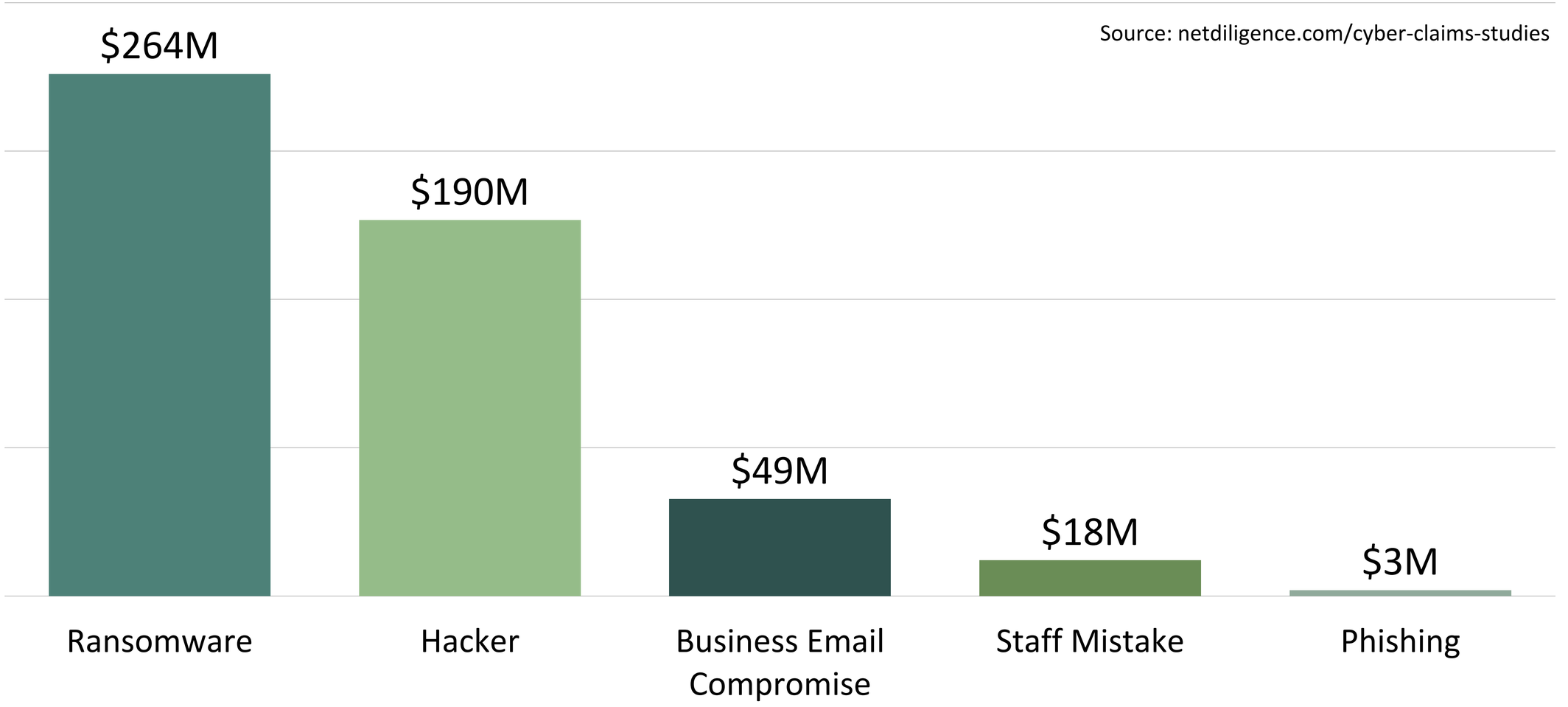
So what does this mean?

1. SME’s are less capable of defending themselves
2. Cache of personal data is high value, easier to access, low risk to criminals
3. Higher probability of under prepared cyber and IT environments
4. Lack of internal controls for privacy data

Source: netdiligence.com/cyber-claims-studies

Cause of Loss

Source: netdiligence.com/cyber-claims-studies



Cyber Liability Coverage

Providers have been consolidating over the last 5 years

- Cingo's access to Cyber Policies meeting our internal criteria has reduced dramatically
  - 13 providers in 2019
  - 2 providers in 2022
- As claims increase, insurers are reducing their cyber liability books
- Cyber liability policies are limited under standard G&L policies
- When covered, providers are limiting coverage to specific breeches

Resolution

Large Organizations

- Allocate significant investment into internal services and technology development to protect the organization.
- Utilize single source products to assist your tech team with deployment
- Cross platform integration must be understood to build the functional architecture
- Seek third party validation from all providers
- SOC2 is the most widely accepted.

SME’s

- Internal tech teams require CE to navigate the evolving market threats
- Necessity to evaluate internal or external providers:
- Independent IT companies have to innovate scalable and affordable solutions for SME’s
- In a regulated space, third party verification such as SOC2, or otherwise should be provided to validate any provider
- Don’t base decision on cost, you get what you pay for.

www.cingo.solutions