Digital Edge

Welcome

“Cyber security is a self defense system. Cyber security is not a technology. It’s an attitude.”

Standards vs Hackers and Lawmakers

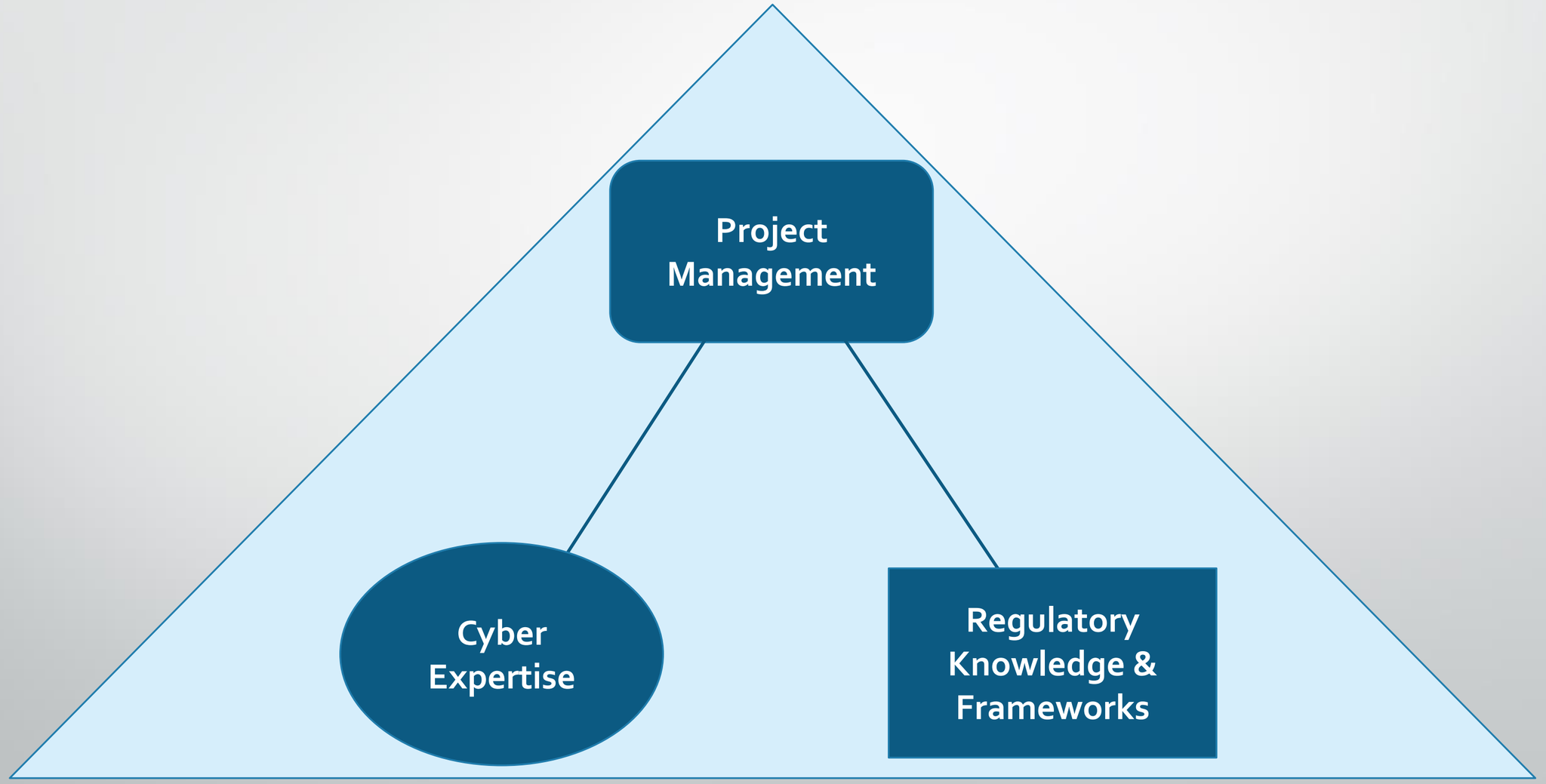
Michael Petrov CEO

Digital Edge

About Digital Edge

- Nearly 25 years in business & we are global
- Nothing is too simple and nothing is too complex
- Assessing and implementing the most efficient way to solve a problem is our hallmark
- We take a team approach and “pass the ball”
- Cyber Security & Cyber Compliance are part of our DNA

The Right Brain vs. the Left Brain



The Landscape Continues to Change Rapidly

- The Cyber Compliance frameworks are becoming increasingly more challenging to obtain certification
- COVID has also played a major role in affecting how companies operate (work from home, laptops vs desktops etc.)
- The hackers are well funded and more and more sophisticated
- Both the simple and the complex issues NEED to be addressed
- How can you “improve your game” to continue to be leading Cyber Security/ Cyber Compliance professional?

Agenda of the day 1

- Introduction
- Who are the bad guys
- Are you smart enough?
- Law system in US
- Federal laws
- Local laws
- Bad guys

Who?

Under Attack – 2 advisories

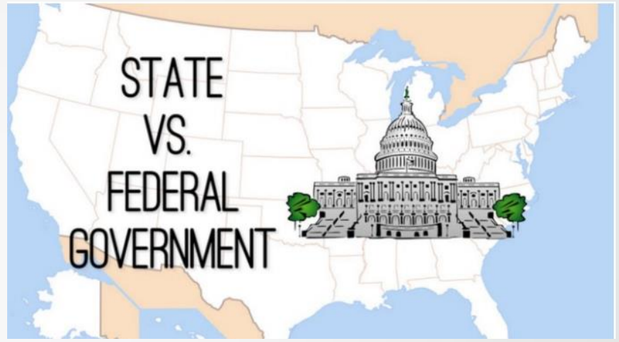
Who are the bad guys?

Cybersecurity and Privacy Laws in the US, Canada and the EU - Introduction

Who am I, and what am I doing here?

My name is Keith Barry, and I joined Digital Edge (DE) in 2013. I am an cybersecurity attorney, and I have also worked over 10 years on the tech side. In addition to a legal background, I have a BA in Computer Science, as well as Network+, Server+ and AWS Cloud Architect certifications. I am DE's VP of Compliance. I assist companies with adhering to laws, regulations, and industry standards.

Cybersecurity and Privacy Laws in the US - I



The US is very large so its legal system is very **complex**.

But, if you're going to be working with a US based company, you will need to have some understanding of the cybersecurity laws that have been put in place.

GENERALLY – The Federal government isn't technically above the state governments. They exist side by side. However, Federal laws have supremacy over state laws *as long as the Federal government has the constitutional authority to make the law.

Feds – May only make a law in an area the US Constitution permits it to make a law. For example – Feds may make laws that deal with **commerce**.

States - Have the general right to make any law. *There are caveats beyond the scope of this presentation.

Cybersecurity and Privacy Laws in the US - II

Federal Laws and Regulations

a. MAY apply to all companies operating within the boundaries of the United States,
b. Constitute the main body of regulatory cybersecurity law within the US.

State Laws and Regulations

a. MAY apply to companies operating within the bounds of a particular State,
b. Constitute a minority of the regulatory cybersecurity laws, BUT
c. Constitute the majority of law regarding PERSONAL suits against companies who have had cybersecurity breaches.

Cybersecurity and Privacy Laws in the US - III

<u>What do US Cybersecurity Laws Cover?</u>

There is no *specific* GDPR-like all encompassing law that is applicable to every company.

US cybersecurity laws and regulations are usually **industry specific**. (For example - Financial/Healthcare/Defense industries are well regulated)

NOTABLE EXCEPTION – The Federal Trade Commission (FTC) has broad authority to prosecute businesses in any industry for insufficient cybersecurity controls. Companies need **reasonable** security controls and must keep their promises of privacy.

Cybersecurity and Privacy Laws in the US - IV

What components of privacy and security are covered in US law?

US laws and regulations can have mandates in one or more of the following areas:

a) **Security controls**,
b) **Breach Notification**,
c) **Privacy Rights**.

Security Controls – Technical and/or procedural mandates that companies must have in place. (Firewalls, AV, IDS/IPS, Incident Response Plans, Awareness Training, etc.)

Breach Notification – Mandates that companies must report security breaches to government entities or other individuals who are affected.

Privacy Rights – Restrictions on private data collection or sharing, and rights that individuals have over their private information (PII/PHI).

Cybersecurity and Privacy Laws in the US - V

Who enforces cybersecurity laws and regulations in the US?

It depends. The enforcing authority is specified in each cybersecurity law itself. The FTC, SEC, DHHS, state Attorneys General are the most common.

What are the penalties for breaking the law?

Various. Depends on the law. Many permit large **fines** and some laws have **criminal** penalties. Also, **injunctive orders** mandating changes to a company's cybersecurity system are often prescribed.

Cybersecurity and Privacy Laws in the US - VI

Here are some examples of laws and regulation mandates you should be aware of:

FTC Act Section 5(a):

a. Industry: All
b. Security Component(s) Covered: Security Controls, Breach Notification, Privacy Rights
c. Mandate(s): **Reasonable** cybersecurity controls in place for company size and data sensitivity. Certain healthcare companies must notify affected individuals, the FTC and sometimes even the media. Promises of privacy of information must be kept.
d. Enforcement: FTC
e. **Max Penalty**: **$43,280** ***per*** violation (**Facebook** was fined **5 BILLION DOLLARS** **in 2019**)

Cybersecurity and Privacy Laws in the US - VII

Law examples continued:

Gramm-Leach-Bliley Act:

a. Industry: Financial
b. Security Component(s) Covered: Security Controls; Privacy Rights
c. Mandate(s): **Reasonable** written cybersecurity controls in place to protect PII. Notice to individuals if PII shared and individuals allowed to opt-out of sharing.
d. Enforcement: FTC, SEC, and others.
e. **Max Penalty**: **$100,000** ***per*** violation.

Health Insurance Portability and Accountability Act (HIPAA):

a. Industry: Healthcare
b. Security Component(s) Covered: Security Controls; Breach Notification; Privacy Rights.
c. Mandate(s): **Reasonable** controls to protect PHI (protected health information). Must inform individuals and possibly DHHS of PHI breaches within 60 days. If over 500 individuals exposed, must notify the prominent media outlets. PHI not shared unless certain circumstances satisfied. Individuals have certain rights to access and control information.
d. Enforcement: DHHS
e. **Max Penalty**: **$50,000** ***per*** violation. Up to **1.5 million** in a year.

Cybersecurity and Privacy Laws in the US - VIII

Law examples continued:

Sarbanes-Oxley Act:

a. Industry: Financial
b. Security Component(s) Covered: Security Controls
c. Mandate(s): **Reasonable** cybersecurity controls in place to protect financial information integrity. Company must report control effectiveness to SEC, and certify financial reports are complete and accurate.
d. Enforcement: SEC
e. **Max Penalty**: **5 million dollars**, and up to **20 years in prison** for CIO and CEO if a willfully false certification. (1 million dollars and up to 10 years in prison if not done willfully)

DFARS (Defense Federal Acquisition Regulations):

a. Industry: Defense
b. Security Component(s) Covered: Security Controls; Breach Notification
c. Mandate(s): **Reasonable** controls specified by NIST (National Institute of Science and Technology) to protect unclassified defense information. Report breaches to DoD within 72 hours, and preserve evidence.
d. Enforcement: DoD
e. **Max Penalty**: **No Set Limit. Can be sued for breach of contract and other causes of action. Also contract termination.**

Cybersecurity and Privacy Laws in the US - IX

Law examples continued:

Children's Online Privacy Act (COPPA):

a. Industry: Child related websites or online services
b. Security Component(s) Covered: Security Controls, Privacy Rights
c. Mandate(s): **Reasonable** cybersecurity controls in place. Must get (actual) parental consent before collecting, using, or disclosing PII of a child under 13.
d. Enforcement: FTC
e. **Max Penalty**: **$43,280 *per* violation**.

FINRA (Financial Industry Regulatory Authority)/SEC Rules:

a. Industry: Financial
b. Security Component(s) Covered: Security Controls
c. Mandate(s): Specific controls required to preserve the integrity and accuracy of financial data. Most notably, retention mandates and WORM needed.
d. Enforcement: FINRA
e. **Max Penalty**: **Unspecified dollar amount. (Wells Fargo fined 4 MILLION for failing to maintain adequate WORM implementation)**

Cybersecurity and Privacy Laws in the US - X

The States:

1. The US has a large government structure consisting of a federal government, state governments, and city and local governments. State governments, and state courts have also been getting involved to a greater degree in cybersecurity.

1. **The New York State "SHIELD" (Stop Hacks and Improve Electronic Data Security) Law** – Is a new law enacted by the NYS legislature. Like the CCPA of 2017, it has a data security section and a data breach notification section.

2. **The data security section states** – that any person or business that owns or licenses computerized data that includes private information of a resident of NY shall maintain reasonable safeguards to protect the security confidentiality and integrity of the ***private information***, including but not limited to disposal of data.

Cybersecurity and Privacy Laws in the US - XI

SHIELD continued - A business or person will be in compliance (but not necessarily out of compliance) IF it (a) Is **already compliant under one of the several stated laws** (ex. HIPPA) OR (b) **Implements a data security program that includes** (i) **Reasonable ADMINISTRATIVE safeguards** such as designating security coordinator, identifying reasonably foreseeable risks, assessing sufficiency of safeguards, performing employee security training, requiring appropriate safeguards in capable provider contracts, constantly adjusting the security program as needed; AND (ii) Rea**sonable TECHNICAL safeguards** such as assessing risks in network and software design, assessing risks in information processing, transmission and storage, detecting, preventing, and responding to attacks or system failures, regularly testing and monitoring the effectiveness of key controls, systems and procedures, AND (iii) **Reasonable PHYSICAL safeguards** such as assessing the risks of information disposal and storage, detecting, preventing and responding to intrusions, protecting against unauthorized access to or use of private information during or after the collection, transportation, or disposal of the information, and disposing of the information after reasonable amount of time.

IMPORTANT NOTE - A 'Small business' complies with the above IF its "security program contains reasonable ADMINISTRATIVE, TECHNICAL, and PHYSICAL safeguards that are appropriate for the size and complexity of the small business, the nature and scope of [its] activities, and the sensitivity of the personal information the small business collects…" (ie. the standard is less for small businesses)

Cybersecurity and Privacy Laws in the US - XII

SHIELD Notification Rule - Any person or business or government agency that owns or licenses data that includes private information **must disclose any breach of security of the system following discovery or notification of the breach to any NYS resident whose private information is reasonably believed to have been accessed or acquired** by an unauthorized individual. The disclosure is to be made in the fastest time possible. (*For people or business that '**maintain**' the data but do not own it, they must disclose breach to the data owner who then follows the above rules).

EXCEPTION: Notice not required IF disclosure was
1) inadvertent AND
2) the person or business reasonably concludes that the info exposure will not result in harm

Cybersecurity and Privacy Laws in the US - XIII

The California Consumer Privacy Act (CalCPA) – is another newer state law like the SHIELD law, but is a much more detailed in the area of individual privacy rights, but somewhat less detailed than the SHIELD law with regard to general cybersecurity practices.

For its Reasonable Security Procedures – The CalCPA simply specifies damages if nonencrypted, or nonredacted information is accessed by anyone without authorization, exfiltrated, stolen, or disclosed **because the security procedures were not sufficient to meet the California duty to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information."**

Privacy Rights – Where the CalCPA shines is in its protections for private citizens' private information. (a) businesses must maintain a homepage website for California consumers, and (b) that website must list all categories of PII the business collected in the previous 12 months. **Furthermore, there must be a "request page" for any verifiable consumer who requests**: (a) the categories of sources from which the personal information is collected, (b) the business or commercial purpose for collecting or selling personal information, (c) the categories of third parties with whom the business shares personal information, or (d) the specific pieces of personal information it has collected about that consumer. **Finally**, the business must promptly disclose and deliver, free of charge to the consumer, the personal information required within 45 days of the request. The information must be delivered by mail or electronically in portable readily useable format.

Cybersecurity and Privacy Laws in the US - XIV

More about selling PII - The business shall not sell personal information about a consumer that has been sold to it by another business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to **opt out**. The website must contain (a) a list of the categories of personal information it has sold about consumers in the preceding 12 months that most closely describe the personal information sold, or if the business has not sold consumers' personal information in the preceding 12 months, the business shall disclose that fact, and (b) a list of the categories of personal information the business has disclosed about consumers for a business purpose in the preceding 12 months, or if the business has not disclosed consumers' personal information for a business purpose in the preceding 12 months, the business shall disclose that fact.

Opting Out - A consumer has the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the consumer's personal information. The business must maintain a **clear and conspicuous link on the business' Internet homepage, titled "Do Not Sell My Personal Information**," which links to a page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer's personal information. Furthermore, the business must maintain a description of a consumer's rights to opt out on the internet homepage.

Minors "opt in" – Businesses must not sell the personal information of consumers if the business has actual knowledge that the consumer is less than 16 years of age, unless the consumer, in the case of consumers between 13 and 16 years of age, or the consumer's parent or guardian, in the case of consumers who are less than 13 years of age, **has affirmatively authorized the sale of the consumer's personal information.** NOTE: A business that willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age..

Cybersecurity and Privacy Laws in the US - XV

Discrimination – Businesses must not discriminate against a consumer because the consumer exercised any of the consumer's rights under this law. This includes (a) denying goods or services to the consumer, (b) charging different prices or rates for goods or services, (c) providing a different level or quality of goods or services to the consumer, (d) suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. **However** -Nothing prohibits businesses from charging a consumer a different price or rate, or from providing a different level or quality of goods or services to the consumer, **if that difference is reasonably related to the value provided to the consumer by the consumer's data.** (ie. if by not having that information the product is not as good)

Incentives – The business IS allowed to offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale of personal information, or the deletion of personal information.

Updates and Awareness – (a) the **CalCPA** should be checked for updates every 12 months and the businesses policy should be changed accordingly, (b) the **notices** on the website should be updated and checked for accuracy every 12 months, (c) any employee or contractor of the business who is responsible for handling consumer inquiries about the business's privacy practices or the business's compliance with the CalCPA must be informed of all requirements, and how to direct consumers to exercise their rights under the CalCPA.

Cybersecurity and Privacy Laws in the US - XVI

Private Cybersecurity lawsuits under the "Common Law" – In the Anglo-American tradition, the "common law" is the ancient judge made law of the land that can be traced all the way back to the middle ages. Injury in the common law gives rise to a "cause of action" which can be heard and adjudicated by a court.

The common law causes of action (for most cybersecurity purposes) are as follows: (a) **Negligence** (a company breached a legal duty that caused foreseeable injury to an individual, (b) **Negligent misrepresentation** (a company failed to exercise reasonable care and supplied false information that cause damages to an individual), (c) **Breach of contract** (A company breached a bargained for promise or promises in a contract), (d) **Breach of implied warranty** (A company's product or services failed to satisfy basic expectations of fitness), (e) **Invasion of privacy** (A company published private facts about individual that are offensive and not of public concern), and (f) **Unjust enrichment** (A company knowingly benefitted from an individual in a manner that was so unfair that basic principles of equity require the company to pay the individual the fair value of that benefit).

Cybersecurity and Privacy Laws in the EU - I

The European Union (EU)has a more clearly articulated and comprehensive data security and privacy legal framework than the US. Most notable is the General Data Protection Regulation (GDPR) law that came into effect in 2016.

The EU views privacy as a **fundamental human right**, and so its requirements for privacy and data security are generally more stringent that requirements in the United States.

US companies who conduct business in the EU need to ensure that they adhere to the clear guidelines set out by the GDPR.

Cybersecurity and Privacy Laws in the EU - II

GDPR (desired) Jurisdiction:

All companies established in the EU AND companies **NOT** established in the EU IF the data it processes is related to either (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, TO such EU data subjects, OR (b) the monitoring of EU data subjects' behavior to the extent their behavior takes place in the EU.

What does the GDPR require?

GDPR:

a. Industry: All
b. Security Component(s) Covered: Security Controls, Breach Notification, Privacy Rights
c. Mandate(s): **Reasonable** cybersecurity controls in place. Must notify government authority within 72 hours of security breach, or, if a high risk, notify individuals without undue delay. Restrictions on PII collection. Individual rights to access and control PII.
d. Enforcement: Government Data Protection Authorities
e. **Max Penalty**: **Up to 20 Million Euros or 4% of global annual turnover** depending on severity of infraction. (Whichever is HIGHER) **British Airways was fined 183 MILLION Pounds in 2018 for insufficient security policies.**

Cybersecurity and Privacy Laws in the EU - III

The EU-US "Privacy Shield" - Dealt with transferring European PII to foreign countries**.**

Transferring Europeans' PII outside of the EU- can be a big problem. Under the GDPR, a company can only transfer PII to a non EU country IF:

a. The nation to which the data is being transferred has been deemed by the European Commission to have "adequate" protection for PII**. (NOTE: the US is NOT one of these nations! Ouch**!);
b. The foreign company has adopted binding corporate rules that impose significant restrictions on PII processing;
c. The foreign company agrees to handle Europeans' data pursuant to standard contract clauses that have been adopted by the EU; or
d. The foreign company agrees to binding and enforceable commitments regarding safeguards and data subjects' rights via an ***approved code of conduct or *certification mechanism**.**

US companies who wanted to process European PII often chose to have an EU **approved code of conduct or certification mechanism**.

Cybersecurity and Privacy Laws in the EU - IV

The certification program that US companies used was called **“Privacy Shield”** which was negotiated and approved in 2016 between the US and EU.

What did Privacy Shield require?

Privacy Shield:

a. Industry: All
b. Security Component(s) Covered: Security Controls, Privacy Rights
c. Mandate(s): US companies must have **Reasonable** cybersecurity controls in place. Individuals have rights to access and restrict use their PII. Non EU based companies being transferred data from a US company that complies with Privacy Shield must also have same level of protection and rights that Privacy Shield requires of US companies.
d. Enforcement: FTC
e. Max Penalty: $43,280 *per* violation or *per* day for continuing violations.

Cybersecurity and Privacy Laws in the EU - V

HOWEVER – THE EU-US PRIVACY SHIELD WAS STRUCK DOWN BY THE EU COURT IN JULY 2020. It is no longer valid. So US companies must try and satisfy one of the other listed requirements for data transfer outside the EU.

Negotiations for a replacement are ongoing. I see a viable replacement as unlikely given that the reason it was struck down is the secret US Government spying on personal data for defense purposes. It is unlikely the US will agree, because that was the main issue at hand for the predecessor to Privacy Shield, and protections for government snooping were not included in the latest Privacy Shield rules.

Why it Matters

IT is no longer the largely unregulated “wild west” component of industry in the US that it used to be.

The laws I have discussed are just a small fraction of the total cybersecurity laws in place in the US at the Federal and State levels.

Even if a company is not directly regulated by a security authority, it is likely that they are in another company’s supply chain that is regulated and part of that regulation is ensuring their suppliers have adequate cybersecurity controls in place.

Privacy and security matter for their own sake. Having a breach could be a public relations nightmare, and will cost you clients. Privacy is important to everyone, and being the kind of company that is known to be trustworthy and secure will outweigh the added expense of implementing a reasonable cybersecurity system.

How to Educate Executives

Focus on risks - Executives need to know that there is a real risk to the company and that the IT field is changing towards being more risk centered and compliance oriented. Let them know about any and all vulnerabilities the company has. Further, they need to know that noncompliance with applicable laws could harm the company in a real way if there is a breach.

Do not exaggerate – the task or cost of bringing your systems into compliance. Determine what steps need to be taken specifically and the cost and time associated with the undertaking. Provide options.

Benefits – Make sure they are fully aware of the benefits of having an implemented cybersecurity system. Inform them of the various certifications that are available and how they can be used to leverage additional business while also satisfying legal and regulatory requirements.

As always – don’t be pushy, and if possible make them think cybersecurity is their idea.