**EMCS2420: Management of IT Systems and Cybersecurity Risks**

Post-Work: Final Paper Assignment

Brian Russel Davis, brian\_davis@brown.edu

#### Overview

While it has been overlooked in many organizations for years, today having a Functional Security Plan is no longer optional. Personally Identifying Information is sought by companies trying to market to consumers and unfortunately it is also sought by attackers who seek to steal and defraud. It is the company’s position that we work individually and collectively to protect this information and disclose breaches in a timely fashion according to International, Federal, State and Local Laws. Furthermore, in order to protect the data, the assets and most importantly the people, we must create a practice of cybersecurity, one formulated and based on the guidance and cumulative experience from government, academic experts and the private sector.

#### Format

This plan is a functional living document with a purpose. That purpose is to infuse Privacy and Security into the activities that take place in the corporate context and to help employees, managers and leadership understand the steps needed to fulfill the company's mission, protect users and obey the law.

#### Recognized Standards and Frameworks

###### NIST

“The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.”[[1]](#footnote-0) NIST for us, is a way to approach the programmatic analysis and response to the incidents that occur in the computing infrastructure. The framework helps us simplify the myriad of tasks needed to run a successful cyber security plan into buckets categorized as: **Identify, Protect, Detect, Respond and Recover**. Much has been written about these steps which are often recognized as a continuous cycle. However not much has been written about who should be performing these tasks and the capacity in which they may execute the tasks needed to fulfill their responsibilities. This plan, using NIST as it’s axiom will explore the ways in which workers our organization expresses their agency.

#### Agile Inspired

This plan is inspired by the Agile Development Standard. Agile helps teams make products that align with tangible needs, whether need emanates from a user or an internal admin. The agile way of speaking lends itself to function or form and usability or style. For example, in Agile we would define a User Story, meaning something a User would say to describe an action they would like to take. The statement relates the Subject, the Action and the Target of the story. “As a User I would like to read about my Data Privacy Rights” Here the subject is this User ( so external to the company ) and the action is being able to read about the target which is Data Privacy Rights. If we use this way of speaking as an index to the plan it provides an easy to understand point of entry to anyone approaching the document for the first time. When approaching the document they simply need to ask “Whose viewpoint would I like to read it from, and what actions am I trying to perform on what target(s)” The product manager would start with an index of *“As a Product Manager I would like to make sure the plans for my new feature are GDPR compliant”.* And engineers start with an index of *“As a Backend Engineer I want to be sure that my encryption standards align with the company’s guidelines.”*  And, by using Natural Language Processing, we can train an AI to collect many ways of stating the same index.

##### Security and Privacy Personas

As with any Agile Plan there are personas that relate to the person who completes the action in the User Story. For this plan we will start with a set of 6:

##### The Compliance Officer

Someone responsible for defining the internal policies and guidelines of compliance and which State, Federal and International Laws apply to the activities of the company. Their main role in this plan is creating guidance in alignment with State, Federal, Local and International Law that others will follow and monitor for.

##### The Product Manager

Someone who is responsible for the creation of products and features used in the execution of the company’s activities. Their main role in this plan is to define products and features in alignment with compliances standards.

##### The Software Engineer

Someone who is responsible for creating products according to the definitions from the product manager and writing, utilizing and managing code, systems, and third party software according to the guidance from the compliance officer.

##### The Security Professional

Someone who is responsible for defining, creating and/or implementing security and confidentiality in the technical environments according to the guidance from the compliance officer.

##### The Human Resource Professional

Someone who is responsible for creating, implementing, executing and maintaining security standards among all personnel according to the guidance from the compliance officer.

##### The Manager

Someone who is responsible for creating, implementing, executing and maintaining security standards among all teams according to the guidance from the compliance officer.

##### The Sales or Marketing Associate

Someone who is responsible for formulation, planning, implementation and/or execution of Sales or Marketing on behalf of the company. In the course of these activities the company may collect data on behalf of the company or third party.

##### The User

Someone who relies on the standards implemented by this plan to ensure personal safety, security and privacy.

#### Data Privacy Principles

These principles are meant to provide overarching meaning to the policies and guidelines contained in the plan.

##### Be Ethical and Empathic

Being ethical and empathic generally means that we treat our users privacy and security with as much care or more than we would treat our own. Complying with laws or regulations but violating the “spirit of” these laws is not good enough. As a company with a strong commitment to ethics we treat our users with respect and by extension respect their privacy.

##### Be Honest and Transparent

Being honest and transparent means that we are not trying to trick our users, hide or misrepresent our business practices. For example, if we intend to sell data, we tell them, and if we don’t tell them we don’t sell it, period.

##### Be Vigilant

Being vigilant means taking a stance in relation to Privacy that makes no assumptions about the confidentiality of user information. Never store sensitive company or customer information on personal devices.

##### Be Frugal

Only collect the data necessary to do the job.

#### Data Security Principles and Baseline Definitions

##### Zero Trust

A Zero Trust Network is a network that operates under the assumption that an attacker could already be inside the network or an insider could be malicious.

##### DBAC over RBAC

Discretionary Based Access Control and Role Based Access Control are common ways approaching access control in an organization. Configuration of these systems in this plan with prioritize discretion over role as misconfiguration of role or the misuse of role based credentials can work in an attackers favor. By prioritizing discretion over role, we are hoping to curb the number of attacks that happen due to escalation of privilege by a user who does not need access.

##### Layered Protection

Becoming dependent on any one part of Security Tools for total protection is a mistake. By

#### Our Assets

###### Digital Assets

One of the most important baseline definitions is our definition of what is a digital asset. We define our digital assets so employees know what things to handle with more care. We also use this definition to configure security tools. The chart below outlines our data assets, the format the data usually appears in, the sensitivity of the data and whether it needs to be segmented away from other data why stored.

|  |  |  |  |
| --- | --- | --- | --- |
| Asset Name | Asset Type | Sensitivity | Segmented |
| **Personally Identifying Information**  From employees, contractors, users or interns. Including but not limited to : Full Name, Social Security Number, Phone Number(s), Addresses, Passport Number, Driver’s License Number. | Structured Data | High | Yes |
| **Anonymous User Surveys, Assessments or Reviews**  Including but not limited to star ratings, free-form text product reviews, feedback on services rendered or conversation threads with customer service representatives. | Structured Data | Medium | Yes |
| **User Logs, Usage Logs**  Including but not limited to device logs, REST API usage, Device Generated Error Logs. | Unstructured Data | High | Yes |
| **Server SSH Credentials**  Including but not limited to credentials used to login to servers | Credentials | High | Yes |
| **Engineering Development Credentials**  Including but not limited to credentials used by engineers to login to servers, development platforms or SAAS products | Credentials | High | Yes |
| **API Credentials**  Including but not limited to credentials used by an application to access a REST API. | Credentials | High | Yes |
| **User Credentials**  Including but not limited to usernames, passwords and access token used to authenticate users. | Credentials | High | Yes |
| **Intellectual Property**  Including but not limited to hardware engineering plans, firmware source code and software source code. | Source Code, Schematics | High | Yes |

###### Physical Assets

Physical Assets are often overlooked when in planning security and privacy. Paper records or files, access to the company’s buildings, badges and office equipment are all important physical assets. The chart below outlines our physical assets, a type classification, the asset sensitivity and the prescribed storage method.

|  |  |  |  |
| --- | --- | --- | --- |
| Asset Name | Asset Type | Sensitivity | Storage Method |
| **Printed Employee Records**  Including but not limited to correspondence to/from employees, copies of employees I-9, W9s and identification. | Printed Records | High | Locked File Cabinet |
| **Printed Corporate Correspondence**  Including but not limited to correspondence to/from regulators, incorporation documents | Printed Records | Medium | Monitored File Cabinet |
| **Printed Corporate Financial Records**  Including but not limited to bank account statements. | Printed Records | High | Locked File Cabinet |
| **Employee Badges**  Including but not limited to employee identification cards. | Property | High | Employee Monitored |
| **Company Building(s) and Office Assets**  Including but not limited to the physical building(s) owned or leased by the company. | Property | High | NA |
| **IT Equipment**  Including but not limited to laptops, desktops, cell phones or network equipment owned by the company. | Property | High | Employee Monitored |

#### Laws and Regulations that Govern Our Business

There are a number of laws that govern the collection, transmission and storage of data. Some of these laws apply broadly and others only apply in special circumstances. The following list is meant as a guideline and is not exhaustive.

##### International

###### General Data Protection Regulation : GDPR

In the case that a user who is a citizen of the European Union sends their information to the company, or moves to the European Union after submitting their information to the company, the user will have the right to redress their information in alignment with the GDPR.

##### Federal

###### FTC Act

The FTC Act regulates the company’s business practices [ details about the parts of the FTC Act that apply ]

###### Biometric Information Privacy Act

Whenever any biometric data is collected and stored about the user, by the company or a third party, we must ensure that the collection, transmission and storage of this information complies with the law.

###### Fair Credit Reporting Act : FCRA

Whenever the user's credit report or background information is used to make a decision about them in relation to the services the business offers we must comply with this law.

###### Telephone Consumer Protection Act : TCPA

All communications with users via telephone and SMS must comply with this Act.

###### Americans with Disabilities Act : ADA

All of the business services offered by the company must be accessible to people with disabilities and comply with this Act.

###### The Controlling the Assault of Non-Solicited Pornography And Marketing Act : CAN-SPAM

Email communication with users must comply with this Act.

###### The Children's Online Privacy Protection Act : COPPA

The company must make a reasonable effort ***not*** to collect data belonging to children. In the case that the company accidentally offers services to children or collects the information of a child, the company must deal with the event(s) in compliance with this Act.

##### State

###### California Consumer Privacy Act : CCPA

California’s privacy law is ***new*** and has many of the same features at the GDPR. The intentions of the Act are to provide California residents with the right to:

* Know what personal data is being collected about them.
* Know whether their personal data is sold or disclosed and to whom.
* Say no to the sale of personal data.
* Access their personal data.
* Equal service and price, even if they exercise their privacy rights.

##### Emerging State Privacy Laws

The most recent state to pass a sweeping consumer privacy and security law was California. It's no surprise that business has been anxiously scanning the landscape to see how this new law impacts the way we formulate and implement security.

*“Privacy has been a hot topic for state legislatures in the first month of the year. Legislators in nine states have introduced draft bills that would impose broad obligations on businesses to provide consumers with transparency and control of personal data. If passed, these laws will impact nearly any type of entity that operates in the state, even if the business has no physical presence in the state. Though the California Consumer Privacy Act (CCPA)—which was passed in the course of a week with little legislative debate—has been criticized for containing provisions that are inoperable, legislators in other states have embraced both the structure and specific language of that law.*

*Of the nine states, six follow the full model established in the CCPA, and two approach only certain issues addressed by the CCPA. The ninth state is Washington, which is debating a privacy bill modeled after the GDPR. A tenth state, New Jersey has a draft privacy bill that was introduced last July but has not moved out of committee.”* [[2]](#footnote-1)

These “copycat” laws may not be enforceable but they create an expectation in the minds of users. One that should not be ignored.[[3]](#footnote-2)

#### Company Security and Privacy Governance

The governance of Security and Privacy at the company will be conducted by the Security and Privacy Council ( SAPC ). The Council shall consist of :

1. **Product Managers** representing each product or service that the company offers
2. **Engineer Managers** from each respective engineering team
3. **Development Engineering Managers** who are responsible for managing the staff that have administrative responsibility for corporate servers, networks and development environments.
4. **Senior Level Managers** representing each business unit ( HR, IT, Customer Service, etc )
5. **Compliance Officers** according to speciality
6. **Security Team Managers** according to speciality or business unit.

The SAPC will meet once per month and prepare a report with all significant security events, milestones and/or decisions.

The SAPC will convene within 12 hours of any major security event.

#### Personas Based Index

##### As a Product Manager

As a **product manager** building a new product or feature I want to make sure the product or feature is secure and protect privacy rights.

As a **product manager** supporting an existing product or feature I want to make sure the product or feature is secure and protect privacy rights.

* Properly identify physical and digital assets as defined in the section “Our Assets” that will be created, altered or exposed in connection with this new feature or product.
* Design high level security and privacy based on the type of asset and it’s sensitivity.
* Work with compliance to write the proper disclosures for the new feature or product.
* Work with security to create ongoing monitoring for the new feature or product.
* Work with security and compliance to create a plan of action if security or privacy is breached in connection with the new feature or product.
* Review the product or feature(s) with the Security and Compliance Team on a regular basis to ensure the security and privacy protections are still adequate.

##### As a Security Professional

As a **security professional** I want to make sure my company’s network has a defense strategy in place.

* Properly identify physical and digital assets as defined in the section “Our Assets” that will be created, altered or exposed in connection with this new feature or product.
* Configure security tools to classify digital assets according to their type and sensitivity.
* Configure access to the assets according to the company’s Discretionary Based Access Control Guidelines.

As a **security professional** I want to make sure I know when an attacker breaches my company’s network or gains access to company data.

* Properly identify physical and digital assets as defined in the section “Our Assets” that will be created, altered or exposed in connection with this new feature or product.
* Configure security tools to classify digital assets according to their type and sensitivity.
* Configure security tools to monitor access logs and notify security staff of any abnormal access.

As a **security professional** I want to make sure I know when a malicious insider misuses the company’s network or illegally moves company data.

* Properly identify physical and digital assets as defined in the section “Our Assets” that will be created, altered or exposed in connection with this new feature or product.
* Configure security tools to classify digital assets according to their type and sensitivity.
* Configure security tools to monitor access logs and notify security staff of any abnormal access.

##### As a Software Engineer

As a **software engineer** I was to make sure I am incorporating security and privacy into the new applications I am building.

As a **software engineer** I was to make sure I am incorporating security and privacy into the existing applications I am supporting.

* Properly identify physical and digital assets as defined in the section “Our Assets” that will be created, altered or exposed in connection with this new feature or product.
* Design and implement encryption according to the company’s data encryption guidelines.
* Design and implement secure transmission pipelines according to the company’s secure transmission guidelines
* Design and implement access according to the company’s data access guidelines
* Design and implement monitoring in collaboration with the company’s security team.

##### As a Compliance Officer

As a **compliance officer** I want to monitor if teams, managers and individuals are in compliance with our standards.

* Properly identify physical and digital assets as defined in the section “Our Assets” that are present in the company’s current suite of products.
* Identify the teams, managers and employees that are responsible for building, maintaining and securing the digital assets in the respective products or services.
* Evaluate the risk associated with digital assets respective to their use in the company’s products or services.
* Train the teams, managers and employees on the proper way to mitigate the risk associated with digital assets used in the company’s products or services.
* Organize and conduct regular meetings to review any security or privacy incidents and the security or privacy of current and new products or services offered by the company.

##### As a Manager

As a **Manager** I want to monitor if teams and individuals are in compliance with our standards.

* Properly identify physical and digital assets as defined in the section “Our Assets” that are present in the company’s current suite of products.
* Identify the team members that are responsible for building, maintaining and securing the digital assets in the respective products or services.
* Participate in training the employees on the proper way to mitigate the risk associated with digital assets used in the company’s products or services.

##### As a Sales or Marketing Associate

As a sales or marketing associate I want to ensure that sales or marketing materials comply with company guidelines and policies.

As a sales and marketing associate I want to ensure that any collection of personal identifying information complies with company guidelines and policies.

##### As a User

As a **user** I would like to know my privacy rights.

As a **user** I would like to know if my personal information is being sold.

* The company will provide a privacy and disclosure statement on the company website, in the packaging for any of the company’s devices and include information about consumer privacy rights with terms of service statements when a user creates an account with the company.
* The company will provide brief TL;DR style disclosures that are easy and quick to read alongside more complete and detailed disclosures.

As a **user** I would like to know if my personal information has been compromised.

The company will communicate with affected users via email within 24 hours after the company has become aware of a data breach.

As a **user** I would like to request a copy of all of my personal information.

* The company will provide contact information on it’s webpage on how a consumer can request their data.
* The company will respond to requests for copies of consumer data within 24 hours.
* The company will require the identity of all people requesting copies of consumer data we verified.

As a **user** I would like to request that my personal information will not be sold.

As a **user** I would like to request that my personal information be sold.

* The company will provide contact information on it’s webpage on how a consumer can request that their data not be sold.
* The company will respond to requests within 24 hours.

As a **user** I would like to request that my personal information be deleted.

* The company will provide contact information on it’s webpage on how a consumer can request that their data be deleted.
* The company will respond to requests within 24 hours.

#### Our Policies

The policies that govern IT practices have been templated and standardized for years. We started this plan with a template and customized the details to fit our uses.[[4]](#footnote-3)

###### Customer Data Collection, Data Sharing Disclosure Policy

The company does not sell, barter, trade or share private consumer data.

Consumer data may be used to power recommendations for third party products or services.

Aggregated and anonymized consumer data may be used to create analytical reports that are shared with or sold to third parties.

Aggregated and anonymized consumer data may be used to create data derivatives that power analytical reports that are shared with or sold to third parties.

Consumer data may be merged with third party data. Any user profile created with merged data is never directly shared, sold or bartered with third parties.

###### Data Retention Policy

**Scope**

* This policy applies to all Company employees who use the corporate computer network to create, edit, or maintain corporate electronic data.
* This data retention policy applies to all computer systems except the corporate electronic mail system. The data retention policy for electronic mail is addressed in the Email Archiving Policy.
* This policy does not apply to the retention of paper records

**Policy**

The following rules define the company’s policy regarding the retention, storage and archiving of corporate electronic data:

For the purpose of this Policy, the phrase “electronic data” refers to all files stored in authorized locations on the network. Authorized locations on the network include, but are not limited to, folders mapped to My Documents for authorized individual users, department-level folders accessed by multiple users, and resources such as the corporate intranet that may be accessed by all company users.

By default, the IT Department will maintain electronic data for a period of sixty (60) days. This rule notifies users that the IT Department backups up corporate data on a rolling, 60-day schedule. The purpose of the backups is to provide operational recovery of electronic data that has been corrupted or accidentally deleted or changed within a 60-day window.

Long-term archiving of data is provided only upon request by the Line of Business and approval by the IT Department. The IT Department will retain corporate electronic data for longer than 60 days only when the owners of the business data submit a written request for a different backup and retention schedule. Enhanced data retention schedules will be reserved for mission-critical systems and systems for which the data retention schedule is dictated by requirements in local, state, federal, or international laws.

**Non-Compliance**

Violating this policy is a serious matter that can lead to disciplinary action up to and including discharge.

###### Data Access Policy

**Scope**

* This policy applies to all Company employees who use the corporate computer network to create, edit, or maintain corporate electronic data.
* This data retention policy applies to all computer systems except the corporate electronic mail system. The data retention policy for electronic mail is addressed in the Email Archiving Policy.
* This policy does not apply to the retention of paper records

Data Handling Policy

**Scope**

* This policy applies to all Company employees who use the corporate computer network to create, edit, or maintain corporate electronic data.
* This data handling policy applies to all computer systems except the corporate electronic mail system.
* This policy does not apply to the handling of paper records

**Policy**

Data shall be handled in alignment with the Company Principles outlined in section xx.

Data should be handled by authorized employees according to the Company's Discretionary Based Access Policy.

**Non-Compliance**

Violating this policy is a serious matter that can lead to disciplinary action up to and including discharge.

Acceptable Use Policy

**Scope**

* This policy applies to all Company employees who use the corporate computer network to create, edit, or maintain corporate electronic data.
* This data handling policy applies to all computer systems except the corporate electronic mail system.
* This policy does not apply to the handling of paper records

Policy

**Non-Compliance**

Violating this policy is a serious matter that can lead to disciplinary action up to and including discharge.

#### Our Guidelines

###### Access Controls

Access to systems, networks or machines that hold sensitive data should be issued on a discretionary basis and based on need. For example, an engineering manager for a team working on Application A doesn’t need to have access to a server that only runs Application B and C. All engineers and engineering managers need not have access to all the company’s servers and data. Access should be granted based on a work based need and evaluated on a monthly basis.

Furthermore, only approved development operation staff may have access to servers that hold production data. Engineering staff should not be granted access to production data, or production servers.

Access logs with a record of who accessed each server and when should be created in an automated fashion for analysis by the security team.

#### Budget Implications

In this plan the primary budgetary concern would be staffing. People with the right skills and experience are the most valuable asset when considering security. This is because security issues often are crisis situations. No one can write a plan that addresses every aspect of a security crisis. The most we can hope for is crisis readiness and the development of crisis readiness as a culture. A team that can proactively respond with confidence and accumen is a team of experienced security minded professionals that draw upon their experience to respond clearly without overreacting. A security crisi can quickly cripple a business. Experienced professional with the right tools and support from leadership will outperform any and all expensive software and monitoring. Finding the right people with extensive experience is not cheap. Here is a list of recommended positions and salary expectations:

Lead Data Security Engineer : $225,000

Lead Infrastructure Engineer: $175,000

Senior Technical Product Manager, Security and Privacy: $175,000

Senior Technical Program Manager, Security and Privacy: $175,000

Senior Cloud Security Engineer: $175,000

Red Team Lead: $150,000

Blue Team Lead: $150,000

Threat Intelligence Analyst: $125,000

Compliance Analyst: $125,000

This combination of engineering, product management, program management and analysis should be implemented with care so the technical concerns, business concerns and user concerns have representative seats at the table.

#### Conclusion : Be Reponse Ready

To summarize, the purpose of this plan is not to provide a framework or a roadmap, but instead to provide a list of intelligent questions from people that representatively have something at stake when security or privacy doesn’t go as expected. Writing up a list of scenarios based responses to security issues may “feel good” and give the appearance that everything is handled, but it’s mostly just “security theater”. There can be no templated responses to security crises, but can be ready to respond.

Being “Response Ready” during a breach means creating a culture that fosters the ability to:

1. Identify problems in real-time
2. Be action-oriented
3. Rely on mind-set and experience to formulate responses
4. Be strategically proactive instead of reactive

Once a breach has been identified the security council, a cross-functional team of security-minded individuals should work together to work through 5 distinct steps:

1. Anticipate … issues, problems, challenges.
2. Mitigate … against these problems, issues, and challenges.
3. Prepare … by setting up a crisis response team that formulates strategy.
4. Implement … new software, policies, and practices.
5. Monitor … the infrastructure using the new information gained from the breach.

In the ANTICIPATE step the team should think through all the parts of the business that will be affected by the breach, i.e. privacy implications, if the breach requires a report to the state, local or federal government, legal liability and most important how does the breach affect users and employees. What will customers expect, what fears will they have once the news gets out to the public, and how will the breach impact the organization’s relationships and reputation? Each one of the points mentioned may be a part of or trigger a domino effect. The security council should additionally categorize these concerns as short-term, mid-term and long-term according to their impacts, potential timelines and whether the concerns affect any thresholds. By thinking through these issues ( in parallel to taking action ) the team will make better decisions and have the ability to communicate in a more comprehensive way that demonstrates credibility. From this point forward, any actions taken by the organization should be paired with clear direct communication.

The MITIGATE step for this type of crisis starts mainly with the security team. Servers, routers, switches, desktops, laptops, printers, fax machines and anything connected to the network need to be reset and restored from back-up. Many times there is a fear that resetting hardware will result in data loss, and it might, but data few hours worth of data loss in most cases might be less consequential than dealing with an Advanced Persistent Threat.

PREPARATION, the next step, seems like a step that should have happened before the crisis, and it should. But, in crisis preparation is also important. A breach doesn’t just happen and get solved all in one day. A breach triggers a series of events that will involve weeks and maybe months of strategic responses. The organization should create a cross-functional crisis response team ( one that maybe includes the members of the security council ) that meets twice a day to discuss new developments and to craft communication. In some high stakes situations, a 24-hour crisis war room may need to be created.

IMPLEMENTATION of mid-term and long term mitigation should be the results of mitigation and preparation. Short mitigation like resetting the hardware should make way for mid-term mitigation like finding the source of the breach, patching vulnerable software, services or hardware and formulating new policies and practices so the same breach doesn’t happen again.

MONITORING should have already taken place, however, in light of the new information derived from the breach forensic analysis, improved monitoring should be implemented to shore up the controls.

Responding to breach doesn’t have to be a business ending event. There is no written plan that can stop a business from experiencing a cyber attack. There is no playbook that can provide all the answers on what to do when a breach happens. Every organization will face different challenges depending on the nature of their business and the circumstances surrounding the breach. However, creating a team that is ready to respond to the crisis with a level-headed experience bred strategy is better than any static playbook.

#### Additional Notes

###### Hawaii (SB 418)

The Hawaii bill has a potentially broader reach than the CCPA because it does not define a business, thus extending applicability to all businesses operating in Hawaii. The bill, oddly, does not specify any penalties for violation and does not include a private right of action.

###### Maryland (SB0613)

Though the consumer rights offered in Maryland’s draft bill are the same as those in the CCPA, there are some notable differences in execution. The deletion right is expansive, allowing consumers to demand deletion of any personal data a covered entity maintains, whereas other states merely allow consumers to demand deletion of data only they have provided; there are also no broad exceptions for a business’s internal use reasonably expected by consumers. The draft Maryland bill does not address data belonging to minors and does not create a private right of action.

###### Massachusetts (SD 341)

Massachusetts’s draft law copies the CCPA, but unlike several other states, rewrites several provisions that were duplicative or vague by using clearer language. The substantive requirements are largely the same; however, Massachusetts has fewer exceptions regarding when a covered entity can refuse to delete data, and prohibits any discrimination or financial incentives where consumers have exercised their rights under the law, including the right to opt-out. Massachusetts would also allow private lawsuits to be brought for any violation of the law.

###### Mississippi (HB 2153)

Mississippi’s draft bill hews so closely to the CCPA that it copies the duplicative statements of access rights and similarly fragments the notice requirements. The enumerated categories of data that constitute personal information are slightly different (for example, probabilistic identifiers are missing). And, the private right of action is not limited to data covered by the breach notification law (which is a separate category of more sensitive data)—any unauthorized access of any personal information could give rise to a lawsuit. Mississippi’s bill died in Committee on February 5, 2019, but we have included it for comparison purposes.

###### New Mexico (SB 176)

Sen. Michael Padilla, D-Albuquerque, the bill’s sponsor, is quoted as saying that in drafting the New Mexico’s Consumer Information Privacy Act, “I tried to throw as much spaghetti on the wall” as possible. Padilla’s spaghetti looks a lot like the CCPA, though more clearly structured. The bill also contemplates a significant rulemaking by the NM Attorney General starting in July 1, 2019, with regulations to be promulgated within a year and updated annually.

###### New York (S00224)

New York’s bill is more like California’s Shine the Light Law, which requires transparency regarding the disclosure of personal data to third parties for marketing purposes, although its obligations are much more onerous. The New York Consumer Privacy Act of 2019 would require covered entities to provide a customer with notice of the categories of information shared with third parties and the names and contact information of all third parties with whom data is shared “prior to or immediately following a disclosure.” Service providers (contracted to perform functions for the business, such as data storage and hosting)) are exempted from the definition of third parties. Consumers would also have the right to access specific pieces of information held by the covered entity.

###### North Dakota (HB 1485)

North Dakota’s minimalist bill contains only one substantive requirement: covered entities are prohibited from disclosing an individual’s personal information to anyone other than the individual without the “express written consent” of the individual. To obtain consent, the entity must send a brief, one to two page summary of its privacy practices to the individual by “mail or electronic mail” and receive an affirmative response. While the other states’ draft bills account for a category of third parties who receive data in the context of providing a service to the primary covered entity, the North Dakota law would not allow for sharing with service providers without this consent.

###### Rhode Island (S0234)

The Rhode Island Consumer Privacy Act of 2019 also takes its inspiration from the CCPA, including listing the access right three times. One notable difference, however, is that the bill does not contemplate a role for the state Attorney General, either in rulemaking or enforcement. Thus, provisions that have been criticized as unclear or inoperable in the CCPA, such as what constitutes a verifiable consumer request and the restriction on differentiation in services where consumers have exercised rights unless “reasonably related to the value provided to the consumer,” would not receive further elucidation.

#### Bibliography

Marmor, Rachel R., et al. “‘Copycat CCPA’ Bills Introduced in States Across Country: Privacy & Security Law Blog: Davis Wright Tremaine.” Privacy & Security Law Blog, Davis Wright Tremaine LLP, 20 Mar. 2020, www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou.

Pearson, Christine M., and Judith A. Clair. "Reframing crisis management." Academy of management review 23.1 (1998): 59-76.

Goldberg, Ed. "Preventing a data breach from becoming a disaster." Journal of business continuity & emergency planning 6.4 (2013): 295-303.

Brown, Hart S. "After the data breach: Managing the crisis and mitigating the impact." Journal of business continuity & emergency planning 9.4 (2016): 317-328.

Ruefle, Robin, et al. "Computer security incident response team development and evolution." IEEE Security & Privacy 12.5 (2014): 16-26.

Lind, G. Ö. R. A. N. "Crisis exercises make for crisis readiness." SVERIGES RIKSBANK ECONOMIC REVIEW (2003): 5-24.

1. NIST Cybersecurity Framework. https://www.nist.gov/system/files/documents/2018/02/06/session\_iii\_-\_barrett\_csf.pdf [↑](#footnote-ref-0)
2. Palmieri III, Nicholas F. "Who Should Regulate Data?: An Analysis of the California Consumer Privacy Act and Its Effects on Nationwide Data Protection Laws." *Hastings Science and Technology Law Journal* 11.1 (2020): 37. [↑](#footnote-ref-1)
3. Marmor, Rachel R., et al. “‘Copycat CCPA’ Bills Introduced in States Across Country: Privacy & Security Law Blog: Davis Wright Tremaine.” Privacy & Security Law Blog, Davis Wright Tremaine LLP, 20 Mar. 2020, www.dwt.com/blogs/privacy--security-law-blog/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou. [↑](#footnote-ref-2)
4. “Computer Equipment Security Policy.” FastITTools, www.fastittools.com/view/it-policies/computer-equipment-security-policy/. [↑](#footnote-ref-3)