plante moran | Audit. Tax. Consulting. Wealth Management.

August 21st, 2020

Staying Secure When Transforming To A Digital Government

Speaker Introduction

Alex Brown

Principal Cybersecurity Practice

Furney.Brown@plantemoran.com

248.223.3396

Security in the Public Sector

Security Breaches Continue….

Hackers exploited vulnerability in Superion's Click2Gov Utility Bill Pay Systems affecting government entities across the U.S.

Over 20,000 records from eight cities in five different states have been offered for sale on the dark web.

Phishing cyberattack used against Florida city

Officials tricked into thinking email from bad actor was legitimate.
City officials confirmed they had paid the faux contractor

City payment services downed in cyber attack

Officials refunded late charges related to downed services.
System was suspended deliberately to mitigate damage

City communications hit in ransomware cyberattack.

Officials remained uncertain about personal information breach

Online payment systems affected; 911 services remained unaffected

Cyber Threats On The Rise

- Ransomware
  - Dramatic year-over-year growth in 2019
  - Most expensive and disruptive

Alabama County Offices to Reopen After Ransomware Attack

Chilton County officials say they don't yet know what information was compromised in the ransomware attack two weeks ago, but around 70 computers were targeted in the cyber incident.

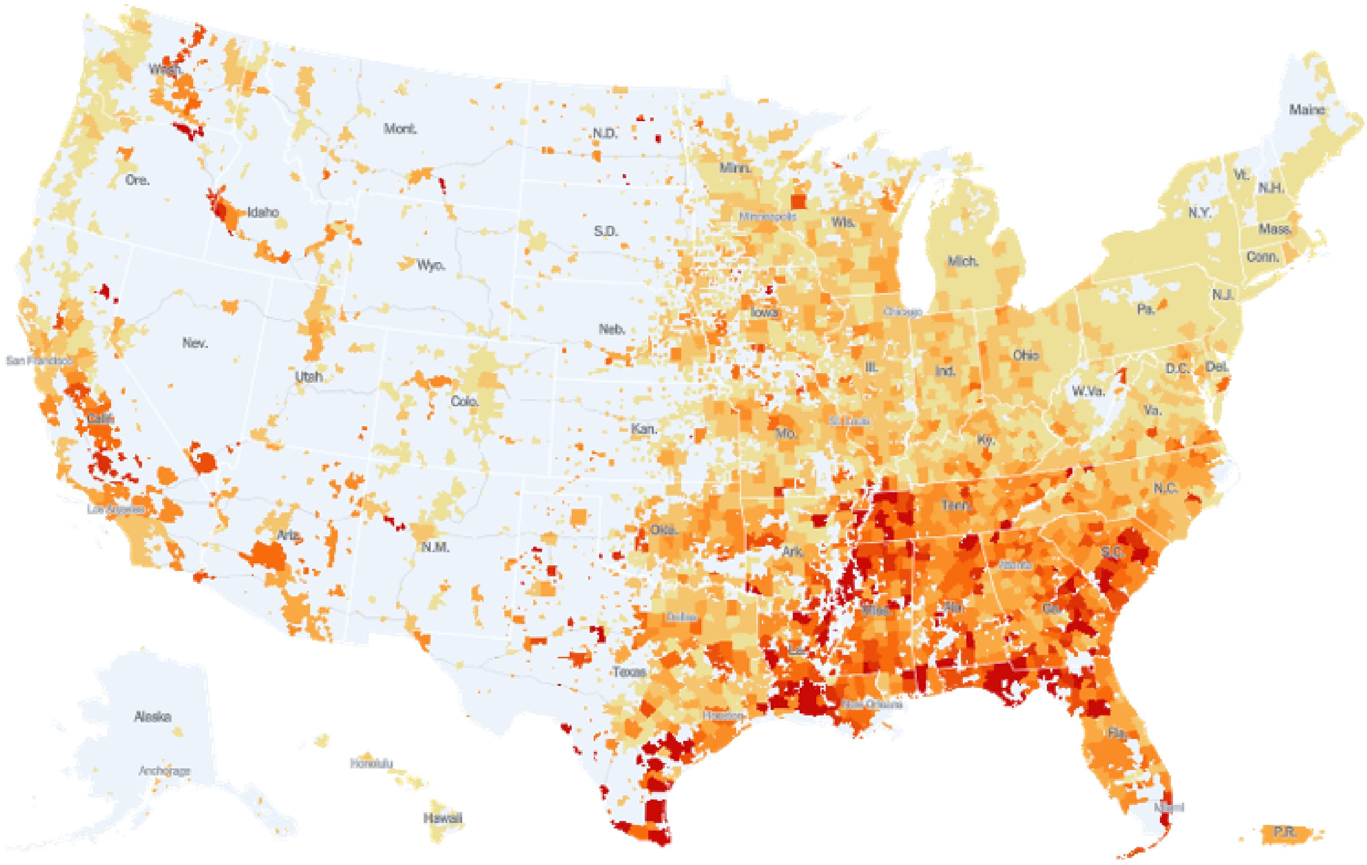
Phishing attacks

- More sophisticated and targeted
- No longer just email

Hacked Washington Schools Platform Sends Phishing E-Mails

Families in Tacoma, Wash., found suspicious emails in their inboxes on Monday after an email platform used by Tacoma Public Schools was hacked, sending 37,600 phishing emails to families, parents and others.

COVID Pandemic Continues to Surge



COVID 19 has added a new challenge to IT security within the public sector. Below are a few examples

- Increase number of remote users
- High demand for remote connectivity
- Risk of data due to user's remote working space (e.g. Zoombombing
- User's technology (e.g. home router)

Increase in Attacks due to COVID-19

Google says it saw more than **18 million daily malware and phishing emails** related to COVID-19 scams just in the past few weeks. That's on top of the more than 240 million daily spam messages it sees related to the novel coronavirus, the company says.

In the midst of the global COVID 19 pandemic that has impacted businesses across the county as well as our daily lives, hackers have seized this opportunity for their personal gain.

Remote work applications like Zoom, Skype, WebEx are starting to become popular themes of phishing lures. This increase has exposed a number of businesses to vulnerabilities from social engineering (e.g. Phishing).

Cybersecurity Trends

Data Breach Stats

4.1	Data breaches exposed 4.1 billion records in the first half of 2019.
71%	71% of breaches were financially motivated and 25% were motivated by espionage.
2,244	Hackers attack every 39 seconds, on average 2,244 times a day.
314	The average lifecycle of a breach was 314 days (from the breach to containment).
48%	48% of malicious email attachments are office files
1 in 36	1 in 36 mobile devices had high risk apps installed.

What makes the public sector an attractive target?

- Security is not often a top (or well- funded) priority
- Governments maintain valuable and sensitive citizen information
- Attacks have been successful

Understanding the Why

- 76% of breaches were financially motivated
- Most cybercriminals are motivated by cold, hard cash. If there’s some way they can make money out of you, they will..
- Most attacks are opportunistic and target not the wealthy or famous, *but the unprepared*.
- Almost three-quarters (73%) of cyberattacks were perpetrated by outsiders. Members of organized criminal groups were behind half of all breaches, with nation-state or state-affiliated actors involved in 12%.
- Over a quarter (28%) of attacks involved insiders. The insider threat can be particularly difficult to guard against—it’s hard to spot the signs if someone is using their legitimate access to data for nefarious purposes.

U.S. Elections Bring Rise to Cyber Activity

Cybersecurity Laws and Policies

Image: This content is subject to copyright.

Cybersecurity Laws Continue To Be Ratified

The legislative sessions for U.S. states in 2019 produced an unprecedented number of new or updated data protection statutes and regulations.

The California legislature passed six different statutes making multiple changes to the California Consumer Privacy Act of 2018 (CCPA). However, the changes were around the edges of the law and the core compliance mandates remain the same for businesses that collect the personal information of California consumers.

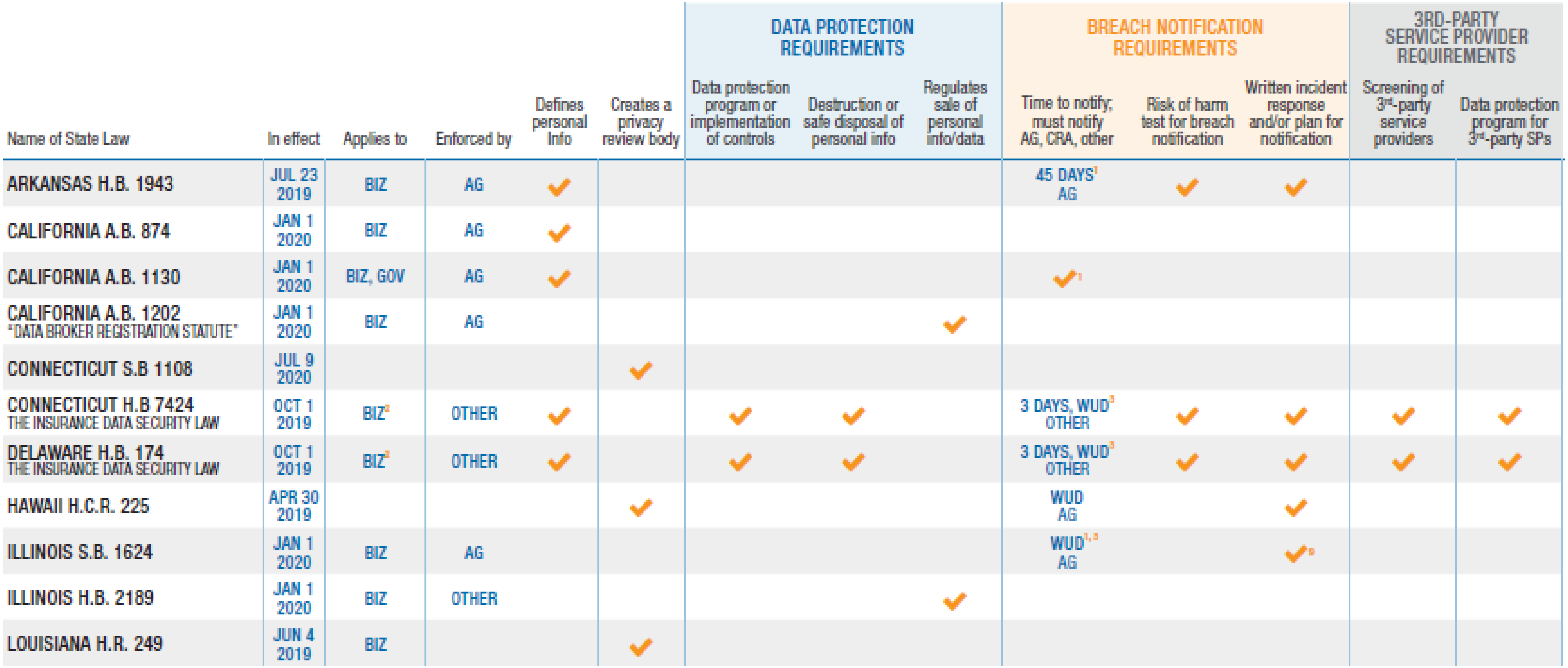
Noteworthy among these new laws are:

(1) New York state’s SHIELD Act, which imposes updated breach notification requirements and information security controls and features wide applicability to businesses and individuals nationwide;

(2) California’s data broker registration statute, the second such statute in the nation; and

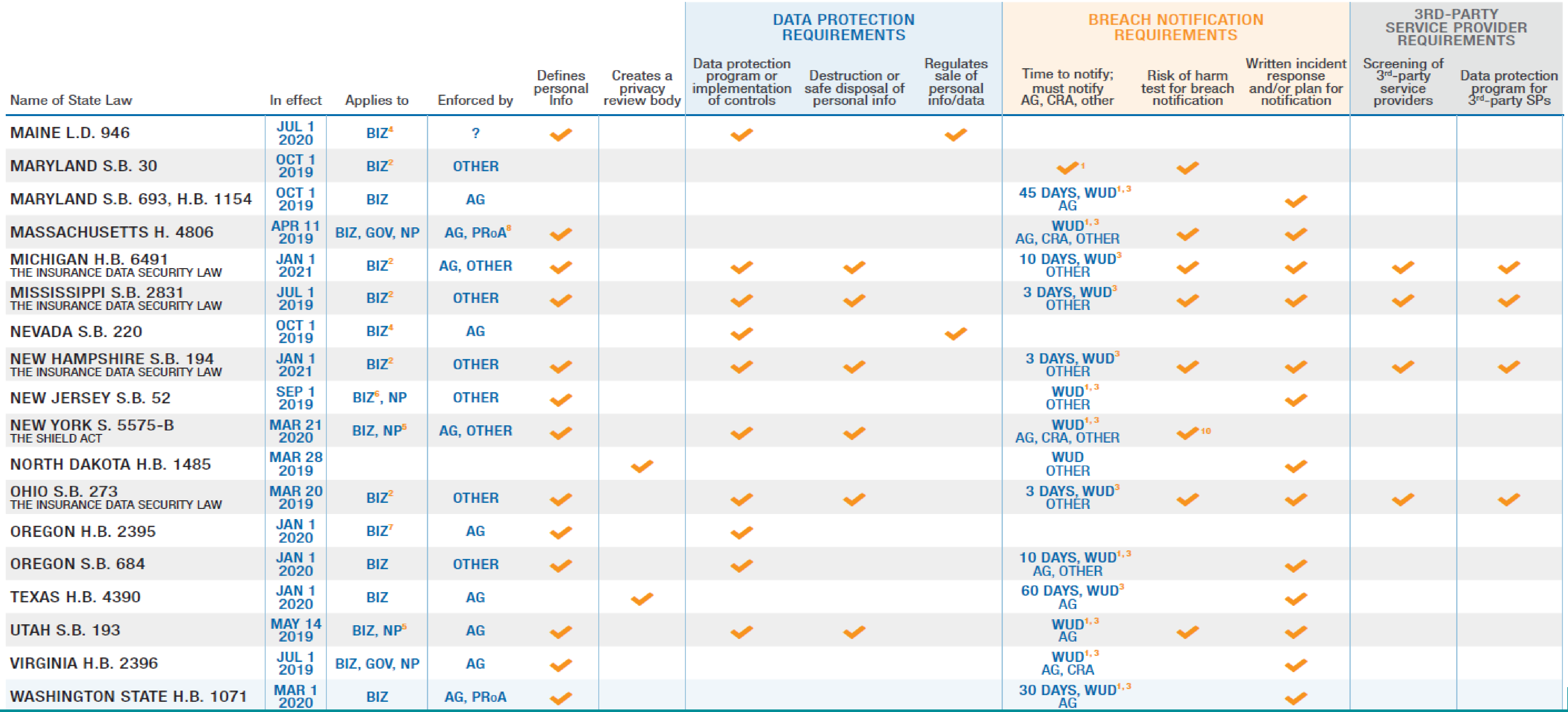
(3) At least six additional state implementations of the NAIC Insurance Data Security Model Law, which is modeled on New York state’s Department of Financial Services Part 500 cybersecurity regulations for financial institutions

New U.S. State Data Protection Laws Enforceable in 2020



						DATA PROTECTION REQUIREMENTS			BREACH NOTIFICATION REQUIREMENTS			3RD-PARTY SERVICE PROVIDER REQUIREMENTS	
Name of State Law	In effect	Applies to	Enforced by	Defines personal Info	Creates a privacy review body	Data protection program or implementation of controls	Destruction or safe disposal of personal info	Regulates sale of personal info/data	Time to notify; must notify AG, CRA, other	Risk of harm test for breach notification	Written incident response and/or plan for notification	Screening of 3rd-party service providers	Data protection program for 3rd-party SPs
ARKANSAS H.B. 1943	JUL 23 2019	BIZ	AG	✓					45 DAYS[1] AG	✓	✓		
CALIFORNIA A.B. 874	JAN 1 2020	BIZ	AG	✓									
CALIFORNIA A.B. 1130	JAN 1 2020	BIZ, GOV	AG	✓					✓[1]				
CALIFORNIA A.B. 1202 "DATA BROKER REGISTRATION STATUTE"	JAN 1 2020	BIZ	AG					✓					
CONNECTICUT S.B 1108	JUL 9 2020				✓								
CONNECTICUT H.B 7424 THE INSURANCE DATA SECURITY LAW	OCT 1 2019	BIZ[2]	OTHER	✓		✓	✓		3 DAYS, WUD[3] OTHER	✓	✓	✓	✓
DELAWARE H.B. 174 THE INSURANCE DATA SECURITY LAW	OCT 1 2019	BIZ[2]	OTHER	✓		✓	✓		3 DAYS, WUD[3] OTHER	✓	✓	✓	✓
HAWAII H.C.R. 225	APR 30 2019				✓				WUD AG		✓		
ILLINOIS S.B. 1624	JAN 1 2020	BIZ	AG						WUD[1,3] AG		✓[3]		
ILLINOIS H.B. 2189	JAN 1 2020	BIZ	OTHER					✓					
LOUISIANA H.R. 249	JUN 4 2019	BIZ			✓								

New U.S. State Data Protection Laws Enforceable in 2020



Name of State Law	In effect	Applies to	Enforced by	Defines personal Info	Creates a privacy review body	DATA PROTECTION REQUIREMENTS			BREACH NOTIFICATION REQUIREMENTS			3RD-PARTY SERVICE PROVIDER REQUIREMENTS	
						Data protection program or implementation of controls	Destruction or safe disposal of personal info	Regulates sale of personal info/data	Time to notify; must notify AG, CRA, other	Risk of harm test for breach notification	Written incident response and/or plan for notification	Screening of 3rd-party service providers	Data protection program for 3rd-party SPs
MAINE L.D. 946	JUL 1 2020	BIZ[4]	?	✓		✓		✓					
MARYLAND S.B. 30	OCT 1 2019	BIZ[2]	OTHER						✓[1]	✓			
MARYLAND S.B. 693, H.B. 1154	OCT 1 2019	BIZ	AG						45 DAYS, WUD[1,3] AG		✓		
MASSACHUSETTS H. 4806	APR 11 2019	BIZ, GOV, NP	AG, PRoA[8]	✓					WUD[1,3] AG, CRA, OTHER	✓	✓		
MICHIGAN H.B. 6491 THE INSURANCE DATA SECURITY LAW	JAN 1 2021	BIZ[2]	AG, OTHER	✓		✓	✓		10 DAYS, WUD[3] OTHER	✓	✓	✓	✓
MISSISSIPPI S.B. 2831 THE INSURANCE DATA SECURITY LAW	JUL 1 2019	BIZ[2]	OTHER	✓		✓	✓		3 DAYS, WUD[3] OTHER	✓	✓	✓	✓
NEVADA S.B. 220	OCT 1 2019	BIZ[4]	AG			✓		✓					
NEW HAMPSHIRE S.B. 194 THE INSURANCE DATA SECURITY LAW	JAN 1 2021	BIZ[2]	OTHER	✓		✓	✓		3 DAYS, WUD[3] OTHER	✓	✓	✓	✓
NEW JERSEY S.B. 52	SEP 1 2019	BIZ[6], NP	OTHER	✓					WUD[1,3] OTHER		✓		
NEW YORK S. 5575-B THE SHIELD ACT	MAR 21 2020	BIZ, NP[5]	AG, OTHER	✓		✓	✓		WUD[1,3] AG, CRA, OTHER	✓[10]			
NORTH DAKOTA H.B. 1485	MAR 28 2019				✓				WUD OTHER		✓		
OHIO S.B. 273 THE INSURANCE DATA SECURITY LAW	MAR 20 2019	BIZ[2]	OTHER	✓		✓	✓		3 DAYS, WUD[3] OTHER	✓	✓	✓	✓
OREGON H.B. 2395	JAN 1 2020	BIZ[7]	AG	✓		✓							
OREGON S.B. 684	JAN 1 2020	BIZ	OTHER	✓		✓			10 DAYS, WUD[1,3] AG, OTHER		✓		
TEXAS H.B. 4390	JAN 1 2020	BIZ	AG		✓				60 DAYS, WUD[3] AG		✓		
UTAH S.B. 193	MAY 14 2019	BIZ, NP[5]	AG	✓		✓	✓		WUD[1,3] AG	✓	✓		
VIRGINIA H.B. 2396	JUL 1 2019	BIZ, GOV, NP	AG	✓					WUD[1,3] AG, CRA		✓		
WASHINGTON STATE H.B. 1071	MAR 1 2020	BIZ	AG, PRoA	✓					30 DAYS, WUD[1,3] AG		✓		

A Few More Facts

- The odds of a data breach today is **1 in 4**, with a 27 percent probability that an organization will experience a data breach over a two-year period.

- The average total cost of a data breach was $3.86 million, up 6.4 percent from last year, and the average total loss for a stolen record was $148, up 4.8 percent from last year.

- In the United States alone, the average total cost of a data breach was $7.9 million, up 7 percent from 2019, and the average cost of a stolen record was $233, up 3 percent.

- For public sector organizations specifically, the total average cost of a data breach was **$2.3 million**, with an average cost of $75 per record.

- The risk factors increasing the chances of data breaches were third-party involvement, compliance failure and extensive cloud mitigation,

Public Sector Cyber Threats

Cyber Espionage

Point of Sale Intrusion

Insider and Privilege Misuse

Malware Attacks

Virus

Lost and Stolen Asset

Social Error

Trojan

Phishing

Web Application Attacks

Ransomware

Payment Card Skimmers

Malicious Insider

Human Error

Denial of Service

Spyware

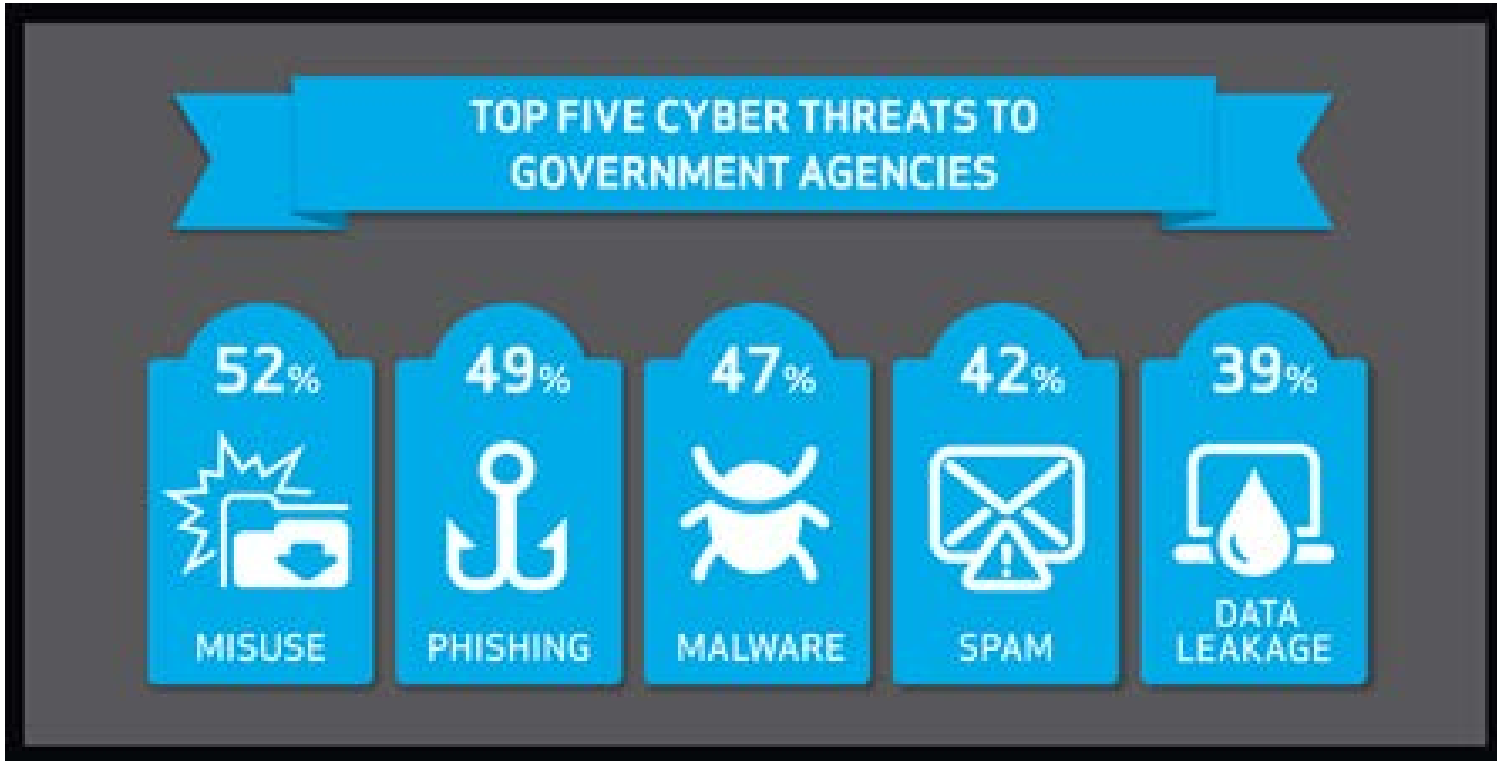
Cybersecurity Can Be Frustrating

- Rising Cost of Breaches
- Increasingly sophisticated hackers
- Widely available hacking tools
- A proliferation of IoT devices
  - We are on route to connect 200 BILLION objects
- Tighter regulations
- Emotional impact to employees

So How Do We Stay Secure In This Ever Growing Digital Environment?

Public Sector Cyber Threats

Top 5 Cyber Threats



Information Security Foundation

Information Security Foundation

- **IT Governance and Policy**
- **Protecting Information**
- **Information Storage and Backup**
- **Information Retention and Destruction**
- **Protecting limited disclosure and sensitive information**
- **Clear Desk / Clear Screen**
- **Locking / logging off your workstation**

Password Policy

- Keep passwords confidential
- Use a pass phrase
- Remember to change your password
- Our #1 defense is our weakest link!

Email (and Internet) Usage Policy

- Internet access for business use
- Email awareness

Mobile Devices

- **Turn User Authentication On –** Make sure screen lock features are turned on, and require a password or PIN to gain entry. There is a ton of valuable data on the device
- **Update Your Operating Systems (OS) Regularly** - If you're using outdated software your risk of getting hacked skyrockets. Vendors are constantly providing security updates to stay ahead of security vulnerabilities.

  Limit Public Wi-Fi - Although it's very tempting to use that free Wi-Fi at the coffee shop, airport or hotel lobby – limit your usage. Any time you connect to another organization’s network, you’re increasing your risk of exposure to malware and hackers.
- **Use a Password Manager-** Not only do they store passwords, they also generate strong, unique passwords that save you from using your cat's name or child's birthday...over and over. It is also highly recommend password managers include Multi Factor Authentication (MFA, also known as 2FA)

Disaster Recovery Plan

- Structured and documented approach for responding to unplanned incidents
- Step-by-step plan that minimizes the effects of a disaster
- Typically, disaster recovery planning involves analysis of business processes and continuity needs
- Disaster Recovery Plan checklist

Working Remotely

Working Remotely

Due to the COVID Pandemic, many companies have decide to have their workforce work remotely. This decision increases the focus of security and ensuring the protection of company data and digital assets.

Below are a few tips to ensure that staff are protecting and appropriately securing sensitive data:

- If staff are using a shared laptop that other family members use too then that device should be treated like a public computer – similar to using a device at a library.
- Save sensitive documents in the appropriate/approved locations – internal file share/SharePoint. Not locally to the computer.
- When printing sensitive documents – what is the policy for securing hard copy documents? Staff should have a draw/cabinet to lock those documents up or shred them immediately

Working Remotely

- Don’t save passwords in browsers using the ‘remember me’ feature
- Another hardware consideration is staff securing their home router
    - Change your router password from the default password
    - Update wi-fi password regularly
- Everyone may not have a business need to access the authority’s internal network and resources, however, when accessing these resources, staff should use a virtual private network (VPN) for a secure/encrypted connection.
- Then there’s a greater reliance on employees to secure their access to cloud application with usernames/passwords

To Sum it All Up

- Prepare. Take time to assess business risks, and know the locations of sensitive data.
- Pay attention to third parties. Understand how vendors use data and ensure they are being as careful as necessary.
- Practice good cyberhygiene. Upgrade and patch software when required.

To Sum it All Up

- Monitor logs. But also determine and select events that are “suspicious and actionable.”

- Encrypt data. Avoid data loss with encryption.

- Train users. Persuade users to do the right thing, and pay attention to insider threats.

- Share stories. Put cyber-risks in terms that shareholders understand.

To Sum it All Up

- Adequate rights. Limit access to the people who need it to do their jobs, and have processes in place to revoke it when they change roles.

- Encrypt sensitive data. By encrypting your data you can render it useless if it is stolen (e.g. Use two-factor authentication)

How can we help you?

Cyber governance

- NIST Cybersecurity Standards
- COSO/COBIT Standards
- SANs Top 20 Security Controls
- Security awareness
- Cyber incident response planning
- BCP/DRP
- 7-point cyber assessment

IT audits

- General controls review (access, physical, operational controls)
- Application controls assessment (SAP, Oracle, PeopleSoft, QAD, Plex, Epicor)
- User access reviews
- ERP security & controls
- Pre/Post-implementation controls review

Security compliance

- Sarbanes-Oxley
- PCI DSS
- HITRUST
- ISO27001 Security Standards
- Financial services regulations (FFIEC, BSA, NACHA, etc.)
- Privacy regulations (HIPAA/HITECH, GLBA, FERPA, GDPR, etc.)

Cyber risk assessments

- Data & application mapping
- Vendor management
- Threat analysis
- Controls mapping
- Maturity models
- Risk-based IT audit planning
- Cybersecurity program

Attack & pen

- External penetration testing
- Infrastructure security assessment
- Vulnerability assessment services
- Social engineering tests
- Web application security
- Database security
- Wireless security
- Virtualization security
- Cloud computing security
- Mobile device security

SOC examinations

- Readiness assessment
- SOC 1
- SOC 2
- SOC 3
- SOC for cybersecurity
- Privacy reviews

Questions?

Thank you!

"Awareness is the greatest agent for change."
— Eckhart Tolle

F. Alex Brown
248-223-3396
furney.brown@plantemoran.com