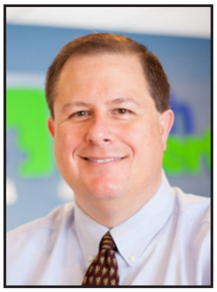
February 2019

TechTidbit.com

brought to you by Tech Experts

Inside The United States Of Cybersecurity



Thomas Fox is president of Tech Experts, southeast Michigan's leading small business computer support company.

Last year, Alabama and South Dakota passed laws mandating data breach notification for its residents.

The passage meant all 50 states, the District of Columbia and several U.S. territories now have legal frameworks that require businesses and other entities to notify consumers about compromised data.

All 50 states also have statutes addressing hacking, unauthorized access, computer trespass, viruses or malware, according to the National Conference of State Legislatures (NCSL). Every state has laws that allow consumers to freeze credit reporting, too.

All 50 states also have statutes addressing hacking, unauthorized access, computer trespass, viruses or malware, according to the National Conference of State Legislatures (NCSL). Every state has laws that allow consumers to freeze credit reporting, too.

While those milestones are notable, there are broader issues when it comes to legislative approaches to cybersecurity across the United States. There are vast discrepancies and differences among states when it comes to cybersecurity protection.

What laws are on the books about cybersecurity?

In 2018, there were more than 275 cybersecurity-related bills introduced by state legislatures in 33 states, Washington, D.C., and Puerto Rico.

The legislative action covers a broad range of cybersecurity topics, including:

- **Appropriations**
- **Computer crime**
- **Election security**
- **Energy and critical infrastructure security**
- **Government and private-sector security practices**
- **Incident response remediation**
- **Workforce training**

For companies, especially those that work across state lines, the variances among state laws creates a challenge in tracking requirements and remaining legally compliant.

For example, while most states require immediate notification of a data breach "without unreasonable delay," the deadlines are varied. Nine states require notification within 45 days, South Dakota allows 60 days and Tennessee allows as many as 90 days.

In addition, most states require written notification while some allow for notification via telephone or electronic notice.

While states have focused much of their recent legislation on data privacy, there are many other components of cybersecurity. Again, there is no uniformity. In fact, most states do not have laws about other important cybersecurity issues:

- Half the states have laws addressing denial-of-service attacks.
- Just five states explicitly cite ransomware in statutes.
- Phishing laws are in place in 23 states and Guam.
- Twenty states, Guam and Puerto Rico have laws regarding spyware.

While broader laws addressing malware or computer trespass may be used to prosecute some of these attacks, the discrepancies further illustrate the different approaches and terminology states use.

What states have strong data privacy laws?

Here are a few examples of states that have strong legal provisions within their cybersecurity and privacy laws:

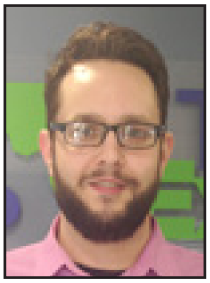
Arkansas: Parental consent is required before student information can be shared with government agencies.

California: The state passed sweeping data privacy laws in 2018 requiring businesses to inform consumers of what personal information is be-

Continued on page 4

Tech Giants Are Branching Into The Medical Field

“The possibilities are endless and Amazon knows that. They are dedicating a lot of time an effort to streamline health services – making a nice profit, but also saving money for the average consumer.”



Jason Cooley is Support Services Manager at Tech Experts.

In early 2018, Amazon announced a partnership with J.P. Morgan and Berkshire Hathaway to restructure healthcare for its combined 1.2 million employees.

This partnership between juggernauts is a stepping stone for Amazon, who has many irons in the fire when it comes to healthcare.

Already, Amazon has been selling medical supplies and equipment. Using partnerships with some of the largest distributors in the U.S., they are making headway and have applied or been approved for all state-by-state licenses needed.

They have also been working on AWS, which is Amazon’s cloud business, to compete with Microsoft Azure and Alphabet’s Google Cloud to provide cloud-based solutions for medical practices and health start-ups.

Amazon’s most exciting prospect in the health field may be Alexa. Amazon’s Alexa has quickly become one of the most used, highest rated, and most reliable voice assistants out there. Amazon has started a partnership with Merck to award $125,000 to the best use of Alexa to battle diabetes.

The idea is exciting, but maybe not as exciting as hospitals experimenting with Alexa. Surgeons may use Alexa to create checklists and sharing important information with discharged patients.

We may see a day where Alexa is the tie-in to our appointments with doctors. Imagine having a digital visit set up by Alexa, using a camera to interface with your doctor, and having Alexa capable of sending your prescriptions to the pharmacy.

The possibilities are endless and Amazon knows that. They are dedicating a lot of time an effort to streamline health services – making a nice profit, but also saving money for the average consumer.

While Amazon has an interesting path and a widespread take on where it can make a difference, Apple is also making some headway.

Apple has started beta use of its health record system. Apple utilizes FHIR (Fast Healthcare Interoperability Resources) in the health record app.

FHIR is technology being used across the country in an attempt to make interoperability and cooperation the standard in healthcare.

First discussed back in 2013, Apple has been working hard to make its own mark. In 2016, Apple acquired Gliimpse, a personal health record company. Apple has used that software, along with FHIR to build out their system.

In 2018, they added EMR data into the phone’s health record and shortly after announced their API would be available to third parties to work on applications that would tie-in with health records.

This has allowed patients to transfer their records to their phone and allows other apps to use that data as well.

Games like Pokemon Go and Oscar utilize the step tracker built in to health records. A restaurant chain called Sweetgreen logs meals ordered into the health record.

Continued use could create endless possibilities for managing our own health.

More than 120 different healthcare companies are part of the beta testing for Apple’s health record.

Much like Amazon, Apple’s ambition does not stop there. Apple also has a similar trajectory to that of Amazon. They believe in a day where there is Telemedicine, virtual appointments, and health information at your fingertips.

These two aren’t the only ones trying to get in on the healthcare game. Of course, tech giant Google is also working on being a large part of future medical developments. Tech and healthcare are both evolving and it appears like they will be on the trip together.

CPU Basics: Multiple CPUs, Cores, And Hyper-Threading

What's a central processing unit (CPU)?

The central processing unit (or CPU) in your computer is the brains of the operation. It's a small computer chip that sits atop the main circuit board (motherboard) of a computer. It performs the computational work, such as running programs or applications.

It's the core of your PC, smartphone, or tablet, and it's what makes the whole device run as it should. At its core, a CPU takes instructions from a program or application and performs a calculation.

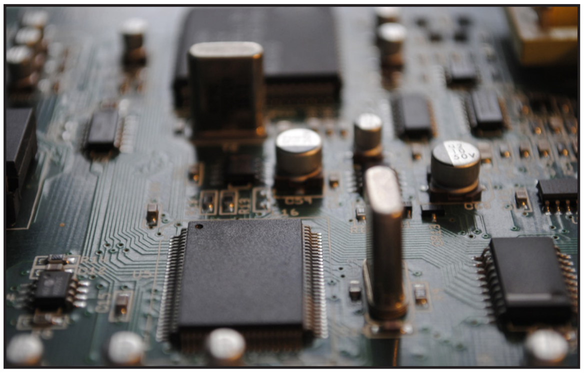
The executed instruction, or calculation, can involve basic arithmetic, comparing certain numbers together, or moving them around in memory.

Since everything in a computer is represented by numbers, those kinds of simple tasks equate to what a CPU does. It's what facilitates everything from starting up Windows to watching a video.

CPU clock speed, or clock rate, is measured in Hertz – generally in gigahertz, or GHz. A CPU's clock speed rate is a measure of how many clock cycles a CPU can perform per second. The clock speed used to be enough when comparing performance.

Things aren't so simple anymore. A CPU core is a CPU's processor. A core can work on one task while another core works on a different task, so the more cores a CPU has, the more efficient it is.

A CPU that offers multiple cores or hyper-threading may perform significantly better than a single-core CPU of the same speed that doesn't feature hyper-threading. PCs with multiple CPUs can have an even bigger advantage.



All of these features are designed to allow PCs to more easily run multiple processes at the same time – increasing your performance when multitasking or under the demands of powerful apps like video encoders and computer aided design (CAD) applications.

What is hyper-threading?

Hyper-Threading (simultaneous multithreading) is a process where a CPU splits each of its physical cores into virtual ones, which are known as threads.

Hyper-threading allows each core to do two things simultaneously. It increases CPU performance by improving the processor's efficiency, thereby allowing you to run multiple demanding apps at the same time.

Multiple cores

Originally, CPUs had a single core. That meant that the physical CPU had a single central processing unit on it. To increase performance, manufacturers added additional "cores," or central processing units. A dual-core CPU has two central processing units, so it appears to the operating system as two CPUs.

A CPU with two cores could run two different processes at the same time. This speeds up your system because your computer can do multiple things at once.

Multiple CPUs

Most computers only have a single CPU. That single CPU may have multiple cores or hyper-threading technology – but it's still only one physical CPU unit inserted into a single CPU socket on the motherboard.

Before hyper-threading and multi-core CPUs came around, people attempted to add additional processing power to computers by adding additional CPUs. This requires a motherboard with multiple CPU sockets.

The motherboard also needs additional hardware to connect those CPU sockets to the RAM and other resources. Systems with multiple CPUs also consume more power.

Systems with multiple CPUs aren't very common among home PCs today. Even a high-powered CAD desktop with multiple graphics cards will generally only have a single CPU.

You'll find multiple CPU systems among supercomputers, servers, and similar high-end systems that need as much number-crunching power as they can get.

> *"It's the core of your PC, smartphone, or tablet, and it's what makes the whole device run as it should. At its core, a CPU takes instructions from a program or application and performs a calculation."*

Inside The United States Of Cybersecurity, continued from page 1

ing collected, disclosed or sold. The law, which goes into effect in 2020, contains provisions giving consumers the right to opt out of having their data sold to a third party.

California is the only state with a constitutional declaration that data privacy is an inalienable right.

Delaware: Recently passed laws restrict advertising to children and protect the privacy of e-book readers.

Illinois: The state is the only one to protect biometric data.

Maine: It's the only state that prohibits law enforcement from tracking people using GPS or other geo-location tools on computers or mobile devices.

Utah: The state is one of only two that requires ISPs to obtain customer consent before sharing customer data.

What states have weak data security laws?

Despite the growing legislative controls on cybersecurity issues and public expectation for data privacy, there are many states that have laws that are lacking, including:

Alabama: There are no laws on the books that protect the online privacy of K-12 students.

Mississippi: To date, no laws exist that protect employee personal communications and accounts from employers.

South Dakota: Companies can retain personal information on employees indefinitely.

Wyoming: Employers can force employees to hand over passwords to social media accounts.

How long does a company need to retain personal identifying information?

Many companies struggle knowing when or if to hold onto personal information on consumers. The challenge is that laws vary greatly from state to state.

As of January 2019, according to the NCSL, only 35 states have laws requiring businesses or government entities to destroy or dispose of this data at all. Of those 35 states:

- Only 14 require both businesses and government agencies to destroy or dispose of data.
- Virginia requires government agencies only but excludes businesses.
- Nineteen states do not require government agencies to dispose of or destroy personal information.

Where is the federal government in cybersecurity?

The federal government has many laws and rules regarding cybersecurity, from HIPAA to the Cybersecurity Information Sharing Act, which allows for the U.S. government and technology or manufacturing companies to share Internet traffic information. Other proposed legislation has hit some roadblocks. Take the Data Acquisition and Technology Accountability and Security Act, which would have established a national data breach reporting standard.

State attorneys general strongly opposed the legislation, introduced in March 2018.

The 32 state AGs argued that the bill would weaken consumer protections, make state laws stronger, and exempt too many companies.

For companies, the variances from state to state present a complex technical challenge. To remain compliant, they need policies, tools and solutions that ensure data is protected and secure.

Managed service providers (MSPs) offer a powerful option to address many data issues. MSPs provide cloud-based, off-site, secure data storage and automated backups. Data, systems and networks are monitored 24/7 to detect and remove unwanted activity.

The advanced firewalls, enterprise-strength anti-virus tools and employee education that MSPs provide help maintain compliance and keep data safe from the attacks that trigger responses.

The growth of state legislation to address cybersecurity issues is welcome. The challenge for companies is finding a reliable solution that allows for responsive and responsible action.

Contact Information

24 Hour Computer
Emergency Hotline
(734) 240-0200

General Support
(734) 457-5000
(888) 457-5001
support@MyTechExperts.com

Sales Inquiries
(734) 457-5000
(888) 457-5001
sales@MyTechExperts.com

Take advantage of
our client portal!
Log on at:
www.TechSupportRequest.com

TECH
EXPERTS

15347 South Dixie Highway
Monroe, MI 48161
Tel (734) 457-5000
Fax (734) 457-4332
info@MyTechExperts.com