What Are The Top Cybersecurity Predictions For 2019?

Several events in 2018 brought cybersecurity to the forefront of public consciousness, as major sectors– from financial institutions to Facebook– were affected by cybercrime. According to Forbes, 34 percent of US consumers had their personal information compromised in 2018. Security experts and business leaders are constantly looking for ways to keep two steps ahead of hackers. As we ring in the new year, predictions for 2019 are a popular topic. Here is what's anticipated this year in the cybersecurity realm.

Tougher Regulations

As digital capabilities are rapidly gaining a worldwide foothold, data is becoming our most highly-valued commodity. Many governments are already recognizing the pressing need to protect citizens' personal information, especially amid mounting pressure from constituents who seek to hold companies accountable. This year will see the rest of the world follow suit, enacting laws that punish corporations and other entities that do not take data security seriously enough. It's anticipated that such legislation will seek to ensure greater protection for connected devices (also known as the Internet of Things or IoT). These measures are also expected to set cybersecurity standards that reflect the value of the protected data.

Stiffer Penalties

Enacting legislation is a step in the right direction, but appropriate consequences are usually needed to enforce it. The EU led the way in taking a firm stand against cybercrime with the GDPR. The Golden State followed with the California Consumer Privacy Act, which takes effect in 2020. These initiatives establish considerable punitive measures for hackers. The UK required Equifax and Facebook to pay maximum fines as mandated by its data protection law. This year, it's predicted that several companies, such as British Airways, Facebook, and Google will come under intense scrutiny, and more jurisdictions are likely to enact stiff penalties– perhaps totaling as much as a billion dollars– for compromising data security.

Consistent Data Breach Patterns

Cybercriminals primarily use email and compromised privileges to access consumers' personal data or engage in other illegal activities, and that trend is likely to remain the status quo in 2019. Businesses and other organizations are advised to put safeguards in place to control privileges and monitor emails, hyperlinks, and attachments.

Cyber Weapon Capabilities Revealed

During the post-World War II era, nuclear war seemed to be the most imminent threat to national security. Today, cyber weapons are believed to carry the greatest potential for harm. Many governments have been developing their cyber arsenal for years, with some using their newfound capabilities to disrupt political systems. Most of these clandestine efforts have been carried out behind closed doors. However, as the threat increases and countries are forced to fine-tune their tactics to defend themselves, they will likely bring their endeavors to light to create a deterrent. Showing hostile governments what might happen should they choose to attack may prevent them from completely unleashing their digital demons– at least for a while. There will likely be outliers who will continue to launch cyber attacks, despite efforts to discourage them. Therefore, companies should do their best to be prepared– developing a proactive, rather than a reactive, strategy.

Continued On Page 3.

Inside The United States Of Cybersecurity

In March 2018, 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.

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 being 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.

Social Media Know-how:

How To Create Org-Wide Groups in Microsoft Teams

As technology improves, so does the way professionals use their programming to increase productivity and efficiency. At one time, emails were the preferred communication between colleagues simply because it was the new form of a written message. Over time, people came to see email as being a bit clumsy for informal messaging, as social media and SmartPhones introduced text messages and chat rooms. You wouldn't send your roommate a formal email to ask whether to pick up an extra coffee on your way home, likewise, it makes more sense to send a text to ask if there are any specific topics to be addressed in the upcoming meeting.

Why Create Teams

The fact is, teamwork relies on communication, and teamwork is a vital aspect of how an office functions efficiently. The definition of your team might vary over time, as it is on one level the entire office staff, but it might also reference your department, or a group of people within that department who are working together on a project. By using Microsoft Teams in conjunction with Office 365, you can quickly choose who to share information with, whether it's a quick message or a formal document. Unlike email, you can easily choose the team to share with rather than sending the message to everybody on your contacts list who doesn't need to know about it, or alternately, accidentally leaving someone out who does need to be informed.

Recommended Settings

Like other software, Microsoft Teams has recommended settings which have proven to work best for most offices. The most common initial setting allows only team members to post to the general discussion. This can allow people outside the team to view what's going on without cluttering up the discussion by adding their own thoughts to a project they may not be working on. Outsiders can still message individual team members with relevant information, and then the member can decide whether it is important enough to post for further discussion. Another way to keep the conversation crisp without unnecessary clutter is to turn off the "@team" notification. Although not a setting, it is important for the team owner to remove accounts that no longer belong, as they no longer need access to your org-wide tem.

Conclusion

Microsoft Teams really is a great new program which is changing the way office communication is handled. Although it is much more than social media, to an extent it uses such a concept to bring the ease of communication such sites have incorporated into a professional setting. It makes it easy to share information with the people who need it, without giving it to people who have no interest or leaving anyone out of the loop who does need to know.

Continued From Page 1.

IoT Working Against Us

Adding to our ever-increasing network of connected devices could have disastrous consequences. It's expected that cybercriminals will be able to program these devices to attack humans. It may sound like the stuff of a dystopian sci-fi novel, but industry leaders predict that 2019 could well be the year that we see people using machines to target other humans to the point of causing great harm or even death. Hackers, for instance, may set programmable thermostats to keep homes unbearably warm or cold, or intentionally cause navigation systems in self-driving cars to suddenly go awry, colliding with other vehicles or striking pedestrians. These incidents could become so widespread that they span entire countries or transcend continents. For now, people still have some control over their devices. Unfortunately, however, more dire predictions are forecast when the day dawns that we surrender such control completely to artificial intelligence (AI).

Multiple Layers of Authentication

In the near future, you may need more than a password to log into your email, social media, and other Web-based accounts. Windows expert Susan Bradley reported to CSO that, "Only using a password to authenticate is increasingly leaving us open to phishing and other attacks." As hackers become more adept at accessing your information, you may be asked to answer additional questions after supplying your password to verify that it's really you. As this will likely prove frustrating for most users, IT providers are seeking a simpler, more sustainable solution.

Of course, with the advancement of technology comes more sophisticated security measures too, so hopefully, these predictions will not be fully realized. It makes sense though, to do everything possible to protect the integrity of your data and ensure that your team is on the same page about the security precautions you plan to take. It's also important to stay current on the latest legislation, standards, and technology to ensure that you're in compliance with applicable regulations and that you have the tools to provide continuous data protection. Utilizing the right strategy will also help you adapt to new developments in data security without disrupting operations or leaving sensitive information vulnerable while you search for appropriate solutions.

February Special

Ready To Fall In Love With Your Technology?

Book Your FREE Cybersecurity Review

And Fall In Love With Your Technology Again.

Hurry, offer good through Feb 28.

Contact us at sales@aveir.com or 775.329.2400
Good until *January 31.*

Quotables

"The best way to make your dreams come true is to wake up."
Paul Valery

"Expect the best. Prepare for the worst. Capitalize on what comes."
Zig Ziglar

Aveir Technology
1400 S. Virginia St. Suite B
Reno, NV 89502
775.329.2400
sales@aveir.com
www.aveir.com

<Insert Presort or Indicia or Affix Stamp Here>

We Have A Special Date Planned For You!

Book Your FREE Cybersecurity Review And Fall In Love With Your Technology Again.

Hurry, offer good through Feb 28.

<First Name> <Last Name>
<Company>
<Street Address>
<City>, <State> <ZIP>