SPOTLIGHT ON

Data Privacy, Retail & Consumer Goods

Your Computers & Privacy: Ready or Not, There They Go

By DAVID LAM

Our right to privacy is being challenged in new and urgent ways. As consumers, we must be aware of the impact our choices have on privacy. As businesses, we must know our obligations to protect Personally Identifiable Information (PII) we collect from customers, employees, and others. This obligation has taken on increased urgency as cybercrime has grown to epidemic levels and it is too easy to access, steal, change, and destroy information.

Concerned with these privacy challenges, in 1995 the European Union led the world in electronic privacy by adopting the European Data Protection Directive. This was replaced in 2018 with the General Data Protection Regulation (GDPR) – which as many of us know, applies to any organization that collects the PII of Europeans.

In 2018 the California legislature passed the California Consumer Privacy Act (CCPA) which went into effect on January 1, 2020. Then, in a bid to strengthen the law, privacy advocates received a major victory when the California Privacy Rights Act (CPRA) was passed in November 2020. Aside from a few provisions, the CPRA goes into effect in 2023.

The CCPA established the requirement for businesses to provide consumers certain notices explaining their privacy practices and gave consumers more control over the personal information that businesses collect about them, including the rights to (among others):

- Know what PII a business collects, how it is used and shared;
- Delete the PII collected from them; and
- Opt-out of the sale of their PII.

For-profit businesses are covered by the CCPA if they meet any of the following:

- Greater than $25 million in annual revenue,
- Buy, sell or receive over 50,000 personal records,
- Receive at least 50% of their annual revenue from selling personal information.

The new CPRA, however, changes the record threshold to 100,000 records and now includes revenue generated from sharing personal information. The CPRA also adds the new category of sensitive personal information.

Included in these laws are the right to have information protected at a commercially reasonable level. Without such protection, both California privacy laws provide for penalties and an ability for individuals to receive compensation.

Business owners may need to adhere to multiple privacy laws which are based on the residence of the individual whose protected data you hold, not only where you do business. Additionally, privacy legislation is being actively discussed nationally, so the principles discussed here may soon apply to many more companies.

One way or another, you are likely to be covered by privacy laws either now or soon. So, it's time to start thinking about what you need to do.

1. Understand your data. It's critical to know what data you have so you can know how to protect it and how to protect the rights surrounding that data.

2. Implement and follow a written privacy policy. Whether you are covered by the new laws or not, other legislation requires privacy policies in multiple situations, and no matter what, you should a) know how you are going to handle private, personal data, even if it's just IP addresses gathered on your website; and b) tell people what you are going to do with their data.

3. Get your information security in order. Both California privacy laws offer defenses to enforcement if you have a commercially reasonable level of Information Security in place. If your firm is large, speak with your Information Security experts to ensure that your practices comply with the law. Otherwise, make sure you have retained qualified Information Security experts to ensure you are protecting your organization. Remember Information Technologist are not Security experts, and you need to consult Information Security subject matter experts who understand what it means to have commercially reasonable Information Security.

4. Develop operational privacy management procedures. Built upon sound privacy policies, effective operational procedures ensure your ability to comply with privacy laws and other contractual responsibilities.

Business owners may need to adhere to multiple privacy laws which are based on the residence of the individual whose protected data you hold, not only where you do business.

Privacy laws are here and will only get stronger. From a privacy perspective, you must ask: Are we employing commercially reasonable levels of privacy and protection now and if new laws are passed – will we still be covered? If the answer to either is 'no,' it's time to get ready.

David Lam, CISSP, CPP, is partner and CISO at Miller Kaplan. Learn more about the firm's information security services at millerkaplan.com.

DATA PRIVACY, RETAIL & CONSUMER GOODS

Best Cybersecurity Practices for Remote Workers

According to recent findings by Proofpoint, cybercriminals are seizing on coronavirus fears by using online scams to extract internet users' personal and financial information. These scams – sent through email, texts or social media – claim to provide coronavirus awareness, sell virus prevention products and/or may ask for donations to a charity. They can often appear to be from a legitimate organization or individual, including a business partner or friend.

"Year round, the National Cyber Security Alliance encourages everyone to be safe and secure online," said Kelvin Coleman, NCSA's executive director. "However, during times of national hardship, such as the coronavirus outbreak, bad actors increase their fraudulent activities. As such, we urge everyone to be extra vigilant against online scams, including phishing and malware, that are more prevalent in times like these."

NCSA offers these tips to avoid being a victim of these scams:

•Don't reveal personal or financial information in an email, and do not respond to email solicitations for this information. This includes following links sent in email.

• Pay attention to the website's URL. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com versus .net).

•If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Contact the company using information provided on an account statement, not information provided in an email. Check out the Anti-Phishing Working Group (APWG) to learn about known phishing attacks and/or report phishing.

•Keep a clean machine. Keep all software on internet-connected devices – including PCs, smartphones and tablets – up to date to reduce risk of infection from malware.

> 'Year round, the National Cyber Security Alliance encourages everyone to be safe and secure online. However, during times of national hardship, such as the coronavirus outbreak, bad actors increase their fraudulent activities. As such, we urge everyone to be extra vigilant against online scams, including phishing and malware, that are more prevalent in times like these.'

Additionally, as more employees are working from home due to the coronavirus outbreak, NCSA urges companies to establish security policies and guidelines for remote workers and train them on these policies and the company's expectations. Companies should also have a clear process for reporting any IT issues for remote workers so they know who to turn to for support.

NCSA recommends the following tips for employees working remotely on how they can stay safe online when using company devices:

Connect to a secure network and use a company-issued Virtual Private Network to access any work accounts. Home routers should be updated to the most current software and secured with a lengthy, unique passphrase. Employees should not be connecting to public WiFi to access work accounts unless using a VPN.

Separate your network so your company devices are on their own WiFi network, and your personal devices are on their own.

Keep devices with you at all times or stored in a secure location when not in use. Set auto log-out if you walk away from your computer and forget to log out.

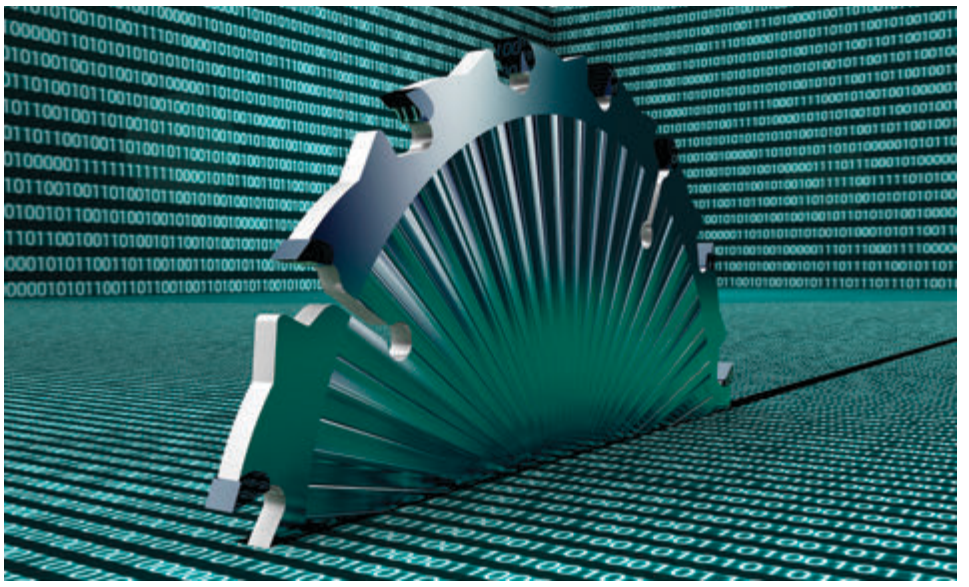
Limit access to the device you use for work. Only the approved user should use the device (family and friends should not use a work-issued device)

Regardless of where you are, NCSA urges all internet users to stay safer and more secure online by updating software on all devices (including antivirus and firewalls) backing up data, enabling multi-factor authentication and having strong, lengthy passphrases for each online account.

For more information and tips on how to stay safe online, visit NCSA at staysafeonline.org.

Responsible Data Destruction Should be Priority #1

By JOHN SHEGERIAN



Data destruction should be on the top of every business' "things to plan" list. If you have papers, storage devices, or electronic items that are no longer needed, you can't just throw them away. You can't ignore the importance of having professional data destruction steps in place. If you haven't thought about how you handle end-of-life devices, you need to.

Go back a little more than 10 years to 2010. At that point, data and information creation was at around two zettabytes. A zettabyte is a trillion gigabytes. Two trillion gigabytes is a lot of information. Now, skip forward to the end of 2020. In just 10 years, the creation of data and information has increased to an estimated 59 zettabytes. This information is stored in clouds, hard drives, USB sticks, and countless other devices.

People often think that restoring an item to factory settings deletes data. Some think that erasing files is enough. That simply removes paths to the information, but it's not destroying the data. Some companies take shortcuts when it comes to keeping records and lists of electronic items being recycled. If your business is deleting data in that manner before giving away or selling old electronics, you are potentially exposing your data to a dangerous breach.

WHAT DATA DOES YOUR BUSINESS STORE?

Any data containing your proprietary company information, your customers' data or employees' personal information must be secured. Before you dispose of old, unused electronics, professional data destruction is essential.

Don't take the chance and destroy the data on your own. Chances are you're not going to do it correctly. If someone steals information that wasn't properly destroyed, not only do you face huge fines, but you also face damage to your company's reputation.

Damage to a reputation is especially important to consider. It's estimated that about 60% of small and medium-sized companies that are impacted by a data breach end up going out of business within six months. Partner with a professional data destruction firm and lower the risk of fines and lost business.

HOW MUCH COULD YOU PAY?

How much can companies pay in fines? It varies. If you manage medical records, improperly destroyed data can violate HIPAA. Fines for HIPAA violations can be as high as $1.5 million.

Financial institutions are bound by the rules of the Fair Credit Reporting Act (FCRA) and the Gramm-Leach-Bliley Act. While FCRA fines can be as high as $3,756 per violation, Gramm-Leach-Bliley Act violations come with penalties of up to $1.1 million. Here are some of the fines levied on companies that violated data destruction and e-recycling regulations.

Affinity Health Plan was ordered to pay fines of $1.2 million back for a 2010 case where the information of more than 344,000 people was found on copier hard drives that the managed care plan provider had leased. When they returned the leased copiers, the information had never been destroyed as per HIPAA rules.

From 2013 to 2015, hundreds of Home Depot stores were caught throwing away batteries, fluorescent light bulbs, paints, and unused electronics. These items were not only going illegally to area landfills, but it's believed that some of the electronic devices may have contained customer information. The company was fined $18.5 million and also had to pay close to $10 million more to help with environmental projects and complying with other measures ordered by the courts.

Morgan Stanley learned the importance of proper data destruction. The company was fined $60 million for failing to have electronic data disposed of correctly during the decommissioning of two data centers. While they'd had a company helping with the decommissioning, they didn't keep track of the data stored on the hardware or oversee where the hardware went. After one warning, the same incident happened several years later, so fines were issued.

Sometimes, fines aren't immediately proposed, but court-ordered actions are imposed. Australia's Commonwealth Bank was found to have lost magnetic storage tapes containing records for upwards of 20 million bank customers. While it believes the tapes were destroyed, the bank didn't get proof of the destruction. As a result, the bank was ordered to improve its security practices and warned that fines would be next if full compliance was not met.

Perhaps most impactful are regulations like Europe's GDPR. Under these rules, multinational corporations are being scrutinized more than ever before for their management of digital data. Inspired by GDPR, many similar new regulations are being put into place here in the US.

If you're not up-to-date on the changing laws, you could make a costly mistake. ITAD providers know the laws and make sure they're always in compliance. It's less hassle for you and makes sure your data destruction project is done correctly.

Make sure you partner with a responsible and certified ITAD provider. Look for certifications from NAID, R2, e-Stewards, and ISO 9001. These four are only given to e-recyclers who pass surprise audits to guarantee they follow laws, use environmentally-responsible practices, and maintain security at all stages of data destruction.

John Shegerian is the co-founder and executive chairman of ERI, the largest fully integrated IT and electronics asset disposition provider and cybersecurity-focused hardware destruction company in the United States. Learn more at eridirect.com.

DATA PRIVACY, RETAIL & CONSUMER GOODS

Cybersecurity Study Highlights Imperatives for State Governments

Continued need for cross-boundary collaboration and increased modernization and digital government services brought to light by COVID-19

Last October, Deloitte and the National Association of State Chief Information Officers (NASCIO) released their 2020 Cybersecurity Study, "States at Risk: The Cybersecurity Imperative in Uncertain Times." The national study is based on responses from 51 U.S. state and territory enterprise-level chief information security officers (CISOs). This is the tenth year of this study and the sixth iteration, with a record number of state and territory CISO's participating this year. The key themes in this year's study are:

- COVID-19 has challenged continuity and amplified gaps in budget, talent and threats, and the need for partnerships.
- Collaboration with local governments and public higher education is critical to managing increasingly complex cyber risk within state borders.
- CISOs need a centralized structure to position cyber in a way that improves agility, effectiveness and efficiencies.

The report also details focus areas for states during the COVID-19 pandemic. While the pandemic has highlighted the resilience of public sector cyber leaders, it has also called attention to long-standing challenges facing state IT and cybersecurity organizations such as securing adequate budgets and talent; and coordinating consistent security implementation across agencies.

These challenges were exacerbated by the abrupt shift to remote work spurred by the pandemic. According to the study:

- Before the pandemic, 52% of respondents said less than 5% of staff worked remotely.
- During the pandemic, 35 states have had more than half of employees working remotely; nine states have had more than 90% remote workers.

"Recent times have created new opportunities for cyber threats and amplified existing cybersecurity challenges for state governments," said Meredith Ward, director of policy and research at NASCIO. "The budget and talent challenges experienced in recent years have only grown, and CISOs are now also faced with an acceleration of strategic initiatives to address threats associated with the pandemic."

"The pandemic forced state governments to act quickly, not just in terms of public health and safety, but also with regard to cybersecurity," said Srini Subramanian, principal, Deloitte & Touche LLP, and state and local government advisory leader. "However, continuing challenges with resources beset state CISOs/CIOs. This is evident when comparing the much higher levels of budget that federal agencies and other industries like financial services receive to fight cyber threats."

> 'The pandemic forced state governments to act quickly, not just in terms of public health and safety, but also with regard to cybersecurity.'

State governments' longstanding need for digital modernization has only been amplified by the pandemic, along with the essential role that cybersecurity needs to play in the discussion. Key takeaways from the 2020 study include:

- Fewer than 40% of states reported having a dedicated budget line item for cybersecurity.
- Half of states still allocate less than 3% of their total information technology budget on cybersecurity.
- CISOs identified financial fraud as three times greater of a threat as they did in 2018.
- Overall, respondents said they believe the probability of a security breach is higher in the next 12 months, compared to responses to the same question in the 2018 study.
- Only 27% of states provide cybersecurity training to local governments and public education entities.
- Only 28% of states reported that they had collaborated extensively with local governments as part of their state's security program during the past year, with 65% reporting limited collaboration.

The 2020 study also revisits the three "bold plays" of the "2018 Deloitte–NASCIO Cybersecurity Study," covering funding, innovation and collaboration, to assess progress on these strategic issues. While CISOs have made progress in the intervening years, more is needed.

The study is based on responses from U.S. state and territory enterprise-level CISOs. CISO participants answered 61 questions designed to characterize the enterprise-level strategy, governance and operation of security programs.

Information for this article was provided by Deloitte. For more information, visit deloitte.com.