New Approaches to Privacy and Security Are Coming

2019 expectations for changes in cyber-security practices and privacy policies

White Paper

Transform IT

Computer Resources of America

Introduction

Data breaches can have devastating effects. Consumers lose trust in businesses that experience breaches of their personally identifying information (PII), often leading to a significant loss in business. But they are also incredibly costly. The European Union took steps to take back consumer control and security of personal data through its General Data Protection Regulation. The regulation was adopted in mid-April 2016 with compliance required no later than May 25, 2018. California has since followed with a similar state law.

In this white paper we summarize:

- **The prevalence of security failures -** We take a look at how often breaches occur within various sectors.
- **The cost of data breaches -** An inside analysis of how a security breach affects costs and spending.
- **Changes expected in 2019 -** CRA looks at what the new approaches of privacy and security are this year.

How Common are Security Breaches?

In just the first six months of 2018, 3,353,172,708 records were compromised. That means that **every second, more than 200 records were being compromised.** It's safe to say, based on this data provided by Gemalto and Breach Level Index, that data breaches are incredibly common. Therefore, knowing what to expect and how to handle any given breach is fundamental to the flow of operations in your business and personal life.

While the number is alarming, what is more alarming is what's found when you take the time to look at the industries affected.

Healthcare saw the highest number of breaches, at 27% of total breaches in the six month span. While it is impossible to declare exactly what data was compromised we know the type of data the average person provides to healthcare providers: financial and medical information, including that about minor children and dependents. These attacks take the form of weaponized ransomware, vulnerabilities due to misconfigured cloud storage buckets and phishing emails (Healthcare IT News). One such phishing hack, in 2017, a hack of a North Carolina-based healthcare system gave a hacker access to three employee email accounts and 20,000 patient records. This is just one example of the high cost of breaches.

The finance sector saw 14% of breaches.

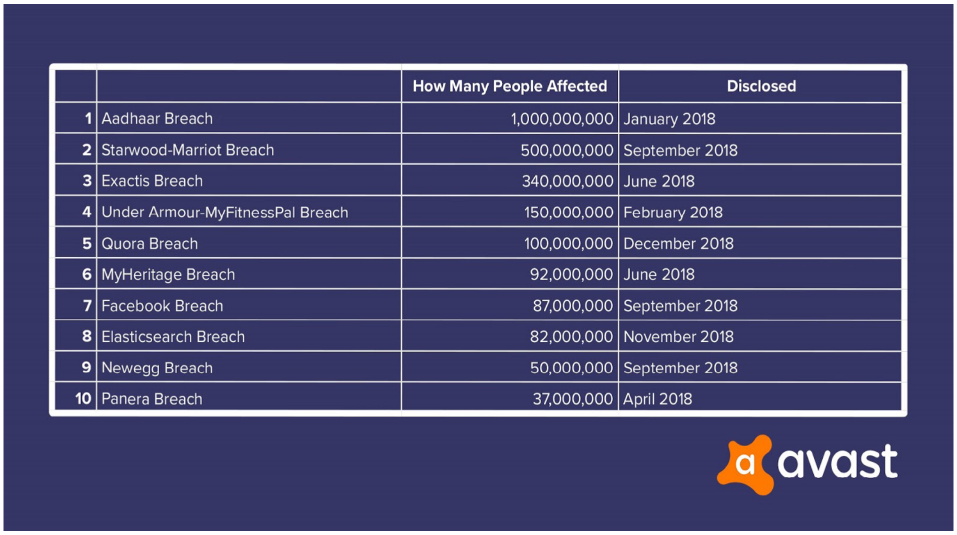
Education was breached 9% of the time. Educational institutions are regularly targeted because of the troves of information they keep on students including financial data.

Professional sites were next at 7%. Again, it's impossible to say precisely what is at risk whether it is work product, staffing information or employee data like salary, bank account information or other data, but the danger is there and should be acknowledged in order to protect data.

Government breaches made up 6% of the total number.

Technology came in at 4% with hospitality and 2% with insurance, entertainment and nonprofits at 1% and social media at less than 1%.

While none of the percentages are overwhelmingly high, these numbers reflect two important considerations for all businesses. First, no sector is safe. Second, 1% of the total records is still nearly 35,000 records. **This data is for just half of 2018, and is 72% higher than the entirety of 2017.**



		How Many People Affected	Disclosed
1	Aadhaar Breach	1,000,000,000	January 2018
2	Starwood-Marriot Breach	500,000,000	September 2018
3	Exactis Breach	340,000,000	June 2018
4	Under Armour-MyFitnessPal Breach	150,000,000	February 2018
5	Quora Breach	100,000,000	December 2018
6	MyHeritage Breach	92,000,000	June 2018
7	Facebook Breach	87,000,000	September 2018
8	Elasticsearch Breach	82,000,000	November 2018
9	Newegg Breach	50,000,000	September 2018
10	Panera Breach	37,000,000	April 2018

Top 10 Biggest Data Breaches in 2018

How Much Do Breaches Cost?

Data breaches are costly. Cyber attacks not only directly affect primary monetary costs but can also cause a decline of income as a result to loss of business, a decrease in client trust and credibility, and also, your company may face potential legal actions from damages. Small to medium-sized businesses are the likeliest targets of attacks so it is crucial to be aware of the types of threats that they may face.

Ponemon and IBM, in a 2018 study, found that globally a breach costs $3.86 million. A breach of 1 million or more records, or "mega breach" costs far more.

The Equifax breach that compromised the personal information of more than 150 million U.S., U.K. and Canadian consumers had run up a bill of $439 million by the end of 2017. Ponemon predicts the final amount will cross $600 million.

Target stated in its 2016 financial report that their 2013 breach, which affected about 110 million people, cost the company nearly $300 million.

Breaches cost more than dollars. Especially for smaller businesses, consumer trust is vital. People will return to Target because they rely on the store, especially college students, recent grads, and families on a budget. SMBs, who are at a far greater risk, are more likely to shutter after a breach.

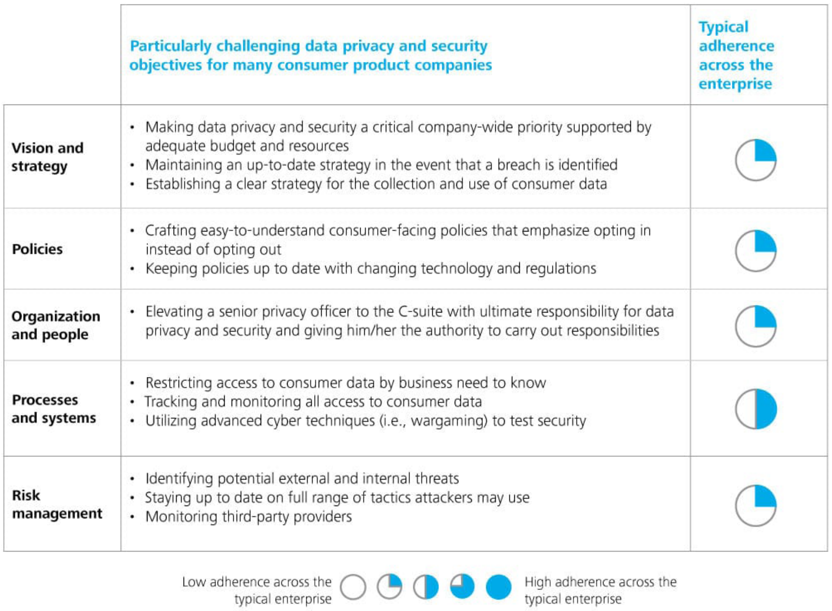
What Changes to Privacy and Security are Expected?

Back in May 2018 the EU's General Data Protection Regulation (GDPR) took effect and set the stage for many other data privacy policies and practices. Data breaches, ransomware, and connected devices security are also in focus as seen in the statistics above, but we expect to see adjustments in cybersecurity practices as cybercriminals reshape concerns.

Compliance

Expect not just more rules, but stricter enforcement of those rules. We anticipate the U.S. developing a law or set of laws similar to the EU's GDPR. This is why many tech and digital marketing sector companies have started recommending aligning sites, networks and other digital platforms with the EU's comprehensive regulations. Best practices include ongoing IT risk assessment, regular auditing ensuring visibility into data repositories and user activities (isBuzz). In addition to new rules, Computer Resources of America expects there to be more pressure for businesses to comply with current standards. One area where this is likely to be seen is notification rules. Several companies have hidden breaches rather than notify those affected, causing nothing short of a digital uproar. SCMP.com reported that Cathay Pacific waited seven months to notify authorities that 9.4 million passenger records had been hacked. The Wall Street Journal shed light on the fact that Google waited six months when 500,000 users had their PII leaked.

Challenge Areas Related to Data Privacy and Security



	Particularly challenging data privacy and security objectives for many consumer product companies	Typical adherence across the enterprise
Vision and strategy	• Making data privacy and security a critical company-wide priority supported by adequate budget and resources • Maintaining an up-to-date strategy in the event that a breach is identified • Establishing a clear strategy for the collection and use of consumer data	◔
Policies	• Crafting easy-to-understand consumer-facing policies that emphasize opting in instead of opting out • Keeping policies up to date with changing technology and regulations	◔
Organization and people	• Elevating a senior privacy officer to the C-suite with ultimate responsibility for data privacy and security and giving him/her the authority to carry out responsibilities	◔
Processes and systems	• Restricting access to consumer data by business need to know • Tracking and monitoring all access to consumer data • Utilizing advanced cyber techniques (i.e., wargaming) to test security	◑
Risk management	• Identifying potential external and internal threats • Staying up to date on full range of tactics attackers may use • Monitoring third-party providers	◔

Low adherence across the typical enterprise ○ ◔ ◑ ◕ ● High adherence across the typical enterprise

Note: See figure 13 for a more complete list of data privacy and security objectives.

Graphic: Deloitte University Press | DUPress.com

State and Federal Statutes Will Increase

California is leading the way for the regulatory wave we expect in 2019. In June, the passage of the Consumer Privacy Act created a much safer digital landscape. The Act, enforceable in 2020, will likely set the bar for federal law. California's law:

- Guarantees users know what data is being collected about them and the reason it is being collected.
- Requires the opt out of the sale of their data to third parties.
- Mandates that children under 16 or their legal guardians must choose to allow the sale of their data.
- Creates portable data by allowing customers to access and download their stored data and then transfer it to a competing service or delete it.
- Makes it illegal for companies to treat customers differently based on whether or not they are willing to have their data sold.
- Provides an avenue for customers to sue companies if there is a breach and the company failed to comply with the law.

More Steps Towards Compliancy

California is not the only state making changes. Other state statutes provide a glimpse into possible 2019 legislative action:

Vermont passed the first law regulating data brokers like Cambridge Analytica. These brokers mine and "keep track of marital statuses, browsing histories, online purchases, debts, housing situations, education credentials" (Slate) and other aspects of users' digital footprints. They then analyze this data and sell it to advertisers to help them increase the value of their ad spends. The data is mined for trends and used to make inferences like someone's health based on pharmacy purchases and can lead to doxing.

All 50 states, and some territories, now have breach notification laws. This includes D.C., Guam, Puerto Rico and the U.S. Virgin Islands.

Arizona, Colorado, Oregon, and Virginia expanded their definitions of personal information and increased third party app oversight.

New Jersey and Rhode Island are seeking laws similar to California's. This, along with House and Senate hearings with Google and Facebook point toward federal law.

AI, Machine Learning and Blockchain Assist in Internet Security

Artificial Intelligence and Machine Learning will play an increasing role across all sectors of information technology but especially in privacy and security. Because AI and ML work together to gather and analyze information and then make predictions, they are the perfect technologies to combat cyber attacks because they generally build from previous attacks using the same strategies. AI and ML are much quicker and less prone to error.

Another technology we've written about this year, blockchain, is likely to become synonymous with internet privacy and security over the next few years. Blockchain eradicates single points of failure and verifies data transactions, leading to greater transparency. 2018 saw the U.S. Food and Drug Administration use blockchain for the real-time exchange of patient data between itself and hospitals. Expect more in 2019.

Security with CRA

Are you ready to implement IT security and privacy practices in your business this year? From managed IT to cloud computing, CRA offers information technology solutions designed with security in mind. Whether you're establishing a new system or revising an older one, CRA is ready to assist you. Contact us to find out how our expert consultants will create the foundation you need to achieve your goals. We are willing to answer any questions that you may have regarding IT security.

CRA™
Transform IT
Computer Resources of America

Corporate Headquarters

64 West 48th Street, New York, NY 10036 – 212-376-4040 – www.consultcra.com – sales@consultcra.com