Beyond Capture & Store: The Future of Compliance

DATA PROTECTION IS THE SINGLE GREATEST RISK TO YOUR COMPANY'S VIABILITY TODAY…AND THE RULES OF THE GAME ARE CHANGING

You've read the news. Historic data breaches continue to make headlines, the costs continue to skyrocket - $3.9m is the cost of the average breach – and the pace isn't slowing, with a record-topping 7.9 billion records exposed through data breaches in the first three months of 2020. The potential for crippling penalties and fines, along with serious threats to customer loyalty and goodwill, threaten the viability of almost every company and register as a source of stress for every CEO and CTO.

Companies have spent the last decade struggling to update processes, technology and training to accommodate the alphabet soup of acronyms such as HIPAA, PCI-DSS, and, most recently, MiFID II, GDPR, and CCPA. We continue to wrestle with the questions that keep leaders up at night: How do we keep customer data safe? How do we comply with the ever-expanding pressure of compliance and regulatory requirements? Are we prepared for an avalanche of customer and auditor requests for information – and the next wave of privacy legislation that solidifies customers' position in the driver's seat?

As cyber-attacks and breaches continue to target high profile companies, new legislation is being introduced across the globe, aimed at changing the rules related to customer data protection and transparency. Keep reading to learn more about how the rules of compliance are changing and how to arm your company to keep pace with emerging compliance requirements.

For more information about compliance-specific applications, read Elevēo white paper: PCI-DSS: A Million Dollar Risk for a 10-Cent Hacking Cost and a blog article Compliance and KPIs.

© 2020

3%

Survey respondents who say GDPR does not apply to them.

DATA PRIVACY BENCHMARK STUDY, CISCO, 2020

Contact center and IT leadership are adept at interpreting long standing compliance requirements, including excluding sensitive customer data from recordings, and storing customer data so it's protected from hackers. The new wave of compliance legislation – MiFID II, GDPR, CCPA, and more to come – goes beyond simple "capture and store" requirements, requiring increased scrutiny over who can access it and how, and how to manage it, anonymize it, delete it, report on it, and export it for customer and auditor inquiries, all within strict deadlines. This is, of course, an expensive endeavor, giving rise to an $88 billion dollar industry and a raft of new technology, responsibilities, and silo breaking processes.

Most of These "New" Laws Don't Apply to Me. Am I Off the Hook?

That is unlikely. First, a recent Cisco survey reveals that only 3% of respondents indicated that GDPR, the European Union's landmark legislation, did not apply to them. Unaffected companies may want to take another look to ensure they have no connections – customers, vendors, employees – within the GDPR radius, to avoid costly misinterpretations.

Even without European business ties, companies with customers, vendors, and employees in the U.S. are part of the global movement of maturing privacy and data protection laws with ever more strenuous, consumer-centered requirements. 2020's California Consumer Protection Act (CCPA), according to industry experts at Cisco, sends a clear signal that we are at "the beginning of a new era in which data is looked at with the same level of scrutiny, care, and risk as anti trust violations and food safety." And while many global organizations are currently covered under the GDPR and CCPA geographic umbrella, proposed legislation is currently under review in five additional U.S. states.

This wave isn't limited to new legislation. Trends point toward an appetite to evolve existing regulations to strengthen consumer data protections and accommodate new technologies. Examples include inviting consumers to weigh in on CCPA interpretation in public forums, and protections for biometric data.

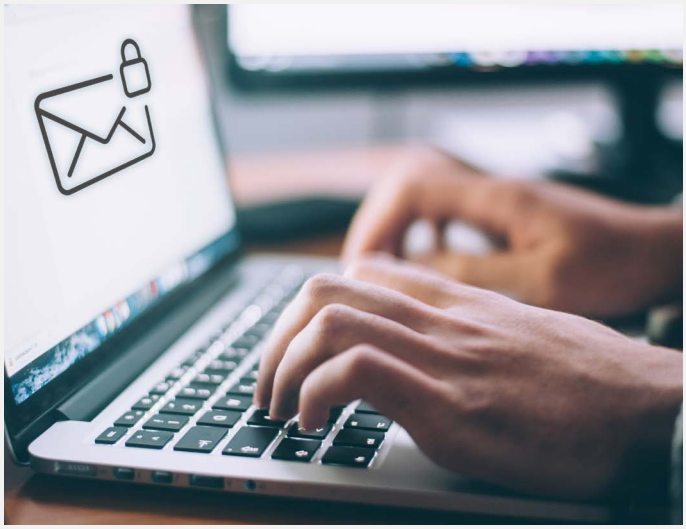
Beyond legal compliance to an investment in privacy

Like most organizations, your compliance strategy is primarily built to avoid financial risk, customer ire and embarrassing disclosures. Most companies are happy to hear that protecting sensitive customer data and improving corporate transparency achieves more than satisfying legal checkboxes. A 2019 analysis of post-GDPR companies found that GDPR-ready organizations experienced a return on their investment: fewer data breaches, with fewer records impacted and shorter system downtime. In addition, more disciplined controls over company assets yield additional benefits for GDPR-compliant companies, including connecting data assets together to increase customer and company value (40%) and boosting understanding of data value (42%).

In addition to direct organizational benefits, an increased focus on corporate transparency improves customers' perception of our organization's trustworthiness. While 75% of consumers believe companies don't take the protection of their data very seriously, customer confidence can be rebuilt through moments of truth where we demonstrate our commitment to safeguard their data and start a dialogue about how that data is used.

© 2020

Are You Ready? Four Critical Questions to Assess Your Compliance Maturity



Rather than relying on patchwork of processes and technology to address a shifting landscape of compliance laws, forward-thinking leaders will stay ahead of the curve by creating a comprehensive, end-to-end data security strategy. This has the added benefit of committing to data protection and transparency as a company differentiator, in an era of daily above-the-fold security breach headlines.

Answer these four questions to determine if your organization is prepared to take on the demands of the next wave of compliance requirements and safeguard your customers' most sensitive data:

Question 1: Do employees handle protected or sensitive information during customer interactions?

In many contact centers, PCI-DSS and HIPAA compliance is achieved with log-established processes and technology. Today, the primary threats to protecting sensitive data are routine changes to contact center technology and processes. A wave of new hires, a missed training day, or a system upgrade can easily leave customers' most private data exposed to damage from careless disclosure or employee malfeasance. While PCI-DSS and HIPAA requirements may not be "new", the damages continue to be steep, and the new wave of compliance legislation establishes more stringent requirements covering how and when breaches must be reported and expends consumers' ability to bring action for statutory damages. Constant vigilance is required.

53%

Companies with sensitive files accessible to every employee.

VARONIS, 2020

Question 2: Do you record and store customer interactions – phone, email, chat, social, text?

When that same sensitive information is recorded – in a call recording or text record – the risk of exposure jumps exponentially. As your organization adds new channels moves into new markets or adds outsourcers staying on top of the compliance basics is essential. Recording and storing audio screen and text details is risky – but it's also critical to training and QA strategies and may also satisfy other compliance requirements such as the MiFID II Dodd-Frank or Sarbanes-Oxley. Customer data storage must be handled with care including excluding sensitive data from recordings through masking or pause-and-resume features encrypting recordings and limiting access to sensitive files to necessary stakeholders.

The first line of defense is to engineer workflows to eliminate unnecessary or redundant discussion of sensitive data or when possible automate processes. Technology solutions can introduce a new set of complications and frustrations and may not reduce risk entirely. As long as we deliver a human-centered experience reps and customers will need to discuss sensitive data during conversations.

87%

Companies storing unnecessary customer data, in a recent study by risk analysts, Varonis.

Question 3: Do you have customers, vendors, or employees in California or the EU? Texas*? Colorado*? Nevada*? New York? * (*pending on publishing date)

If so, your compliance responsibilities no longer end at the walls of the contact center. Emerging enterprise-wide compliance requirements do more than shift the compliance landscape from "capture and store" to a more comprehensive view of end-to-end customer (and employee) data protection. They fundamentally change how organizations manage and monetize what's become one of the most valuable corporate assets: customer data.

Examples include:

MiFID II: EU financial institutions must provide customers with recordings on demand, which translates into secure archiving of recordings across all channels, redundancy and accessible retention rules scenarios, powerful search options, and secure access-rights management. These requirements lead companies to focus on powerful technology to deliver on rigorous customer access to data rights.

GDPR: Customers' rights to be informed, of access, and to be forgotten require a complex net of training and performance management, processes, technology, back office and contact center resources to ensure employees are equipped to respond to customers and auditors quickly and with the required information in a transferable file format.

CCPA: Organizations doing business in California must act on customer requests to know how their data is being stored, used, or sold and to prohibit use of that data on request. This requires an enterprise-wide accounting of data assets and an audit of how Personally Identifiable Information (PII) is handled and secured in systems across the organization. This legislation requires many organizations to manage their data assets more purposefully and strategically.

Question 4: Do you follow the data privacy and security legislation pipeline – and predict what's next for your business?

Not sure what's next? Dive into CCPA and GDPR requirements, and identify the customer data you currently store which may be considered worthy of protection and transparency. Consumer protections under both GDPR and CCPA include the customers' right to know, the right to opt out and the right to delete. What are the process and technology solutions needed to respond to these customer inquiries and requests? What training and tools would your agents need to respond to these requests in a way that builds customer confidence? How will you supply auditors with evidence of compliance? This work requires cross-functional collaboration to identify data assets from across the organization and to ferret out weak workflows, such as legacy systems which store vulnerable and "unnecessary" customer data.

Elevēo's Unique Approach to Solving Complex Compliance Challenges

At Elevēo, we understand the data security threats contact centers face. We've developed impactful and cost- effective solutions that provide IT and CX leaders with the tools they need to go up against threats to customer confidence and the bottom line - and to support easy data access to the people who need it, and safeguards against the people who don't. Over the lifespan of the Elevēo suite of products, our platform has supported compliance regulations and encryption technologies including advanced password management, key management for data at rest, AES/DES/Blowfish encryption algorithms, SSL for data in transit, PCI-DSS system checks and more.

ELEVĒO COMPLIANCE SOLUTIONS		
RECORDING SOLUTIONS	Call, Chat, Email, Video, Screen recording	Capture, encrypt and protect recorded customer interactions to satisfy compliance requirements such as Sarbanes-Oxley.
	Pause and Resume (PR)	Pause audio recordings while sensitive data is shared, and then resume recording. Satisfies common recording regulations.
	Open APIs for PR	Send requests from any authenticated client or service to manage recording pause and resume, and accept call tags with contact center customer metadata.
	Manual PR connectors, CRM toolbar for Cisco Finesse, Salesforce.com	Protect sensitive data from recordings while providing agents with the flexibility to act when a recording needs be paused and resumed.
	Automatic PR connectors for Epic Systems, Pegasystems	Reduce the risk involved in manual pause and resume with hands-off automated business rules.
REGULATION-SPECIFIC SOLUTIONS	PCI-DSS, HIPAA Solutions	Secure recording, encrypted storage, pause and resume solutions.
	MiFID II Solutions	Capture relevant interactions with tagging, audit for data flow and access, export for audit logs with media files.
	GDPR, CCPA Solutions	Comply with data removal rules and features fully integrated into our suite of products contact centers and back office teams

In addition to the security features that are integral to the platform, Elevēo offers an ever-expanding portfolio of solutions to support contact centers' toughest compliance challenges:

What Next? Solutions to Protect Your Company's Two Most Valuable Assets

You need a suite of tools to ensure that you can satisfy current "capture and store" compliance requirements and a set of specialized tools and workflows to support emerging compliance requirements and drive customer goodwill. Your organization needs trusted compliance solutions that are easy to deploy and use across your entire business. Contact us today to learn how Elevēo can help you protect two of your company's most valuable assets: your customers' data and their confidence.

About Elevēo

Elevēo was formed to provide effective, simplified solutions for complex contact center problems.

Our products provide only features needed to elevate contact center operations & processes, are built using modern frameworks and cloud-native technologies that scale & move with your business.

Elevēo products are birthed from ZOOM International with its rich WFO history and award-winning products, services and reputation for service.

© 2020