RSA

WHITE PAPER

GDPR: What It Means To Your Cybersecurity Strategy

Introduction

Modern IT, especially cloud and mobile technologies, has significantly improved access for users from anywhere to anywhere. Whether a user is working remotely and needs to access company systems; taking advantage of 24hr banking to manage their finances; or buying online to avoid shopping crowds; people have amassed a multitude of online "identities" in their effort to improve efficiencies of many day-to-day tasks. Users are not just employing one device, in fact, they typically intermingle an assortment of corporate-issued and personal devices.

Essentially, Modern IT is designed to create cost efficiency and con venience around communications and transactions. The complication is that these benefits are not limited to the organizations and their authoriz ed users but extend out to hackers/cyber criminals. The plethora and intermingling of both personal and company-issued devices added to the swelling number of cloud applications has massively enlarged the attack surface increasing the complexity of protecting an organization while at the same time decre asing the difficulty for compromise.

While organizations try to create friction for unauthorized users by adopting best-in-class technology and hiring skilled cybersecurity professionals, the European Union (EU) has announced a regulation that is "designed to harmonize data privacy laws across Europe, protect and empower all EU citizens data privacy, and to reshape the way organizations across the region approach data privacy." While the EU has had data privacy laws since the 1980's, this is the first regulation that applies directly to organizations established outside the EU that process EU citizen personal data. The GDPR will be a game-changing regulation because it is basically resetting the best practices model for data privacy and protection, globally as the first pan-EU law that is also extraterritorial.

What is the General Data Protection Regulation (also known as the "GDPR")?

The General Data Protection Regulation is a new piece of legislation that is scheduled to become effective in May 2018. This single Europe-wide regulation removes the complexities that organizations currently face around complying with multiple local data protection rules across the EU. Prior to GDPR, each of the

28 member states were permitted to interpret the existing rules in their own way, making compliance across the region complex and expensive.

The GDPR unifies EU data protection legislation. That, in turn, unifies processes and legal obligations for any organization doing business with more than one EU state.

The scope of the GDPR, however, substantially increases the obligations on organizations that are processors of EU citizen personal data. The penalties for non-compliance are substantial, which will propel data protection as a business risk directly into the boardroom.

Why is it necessary?

New technologies and globalization have transformed how organizations collect, access, and use information, including personal data. However, until the formation of the GDPR there were no consistent rules for managing personal data. In fact, even the 1995 Data Protection Directive, which was adopted by the member states of the EU, had inconsistent interpretations, resulting in divergent enforcement practices.

More than 90 percent of Europeans say they want the same data protection rights regardless of where their data is processed. So in January 2012, the European Commission in Brussels proposed a reform of the EU's 1 995 data protection rules to "make Europe fit for the digital age." As such, the Commission pursued a regulation (one law that applies equally) rather than a directive (a law that member states can interpret individually). With this new regulation, the EU believes that they can eliminate fragmentation and create what has been termed a "one-stop shop" for data protection in Europe.

On 15 Dec. 2015, the European Parliament, the European Council, and the European Commission reached an agreement on a joint proposal for the new data protection regulation to establish a modern and harmonized data protection framework across the EU.

What does the GDPR expect to accomplish?

The fundamental aim of the reform is to better protect the rights of individuals regarding their personal data. The GDPR defines personal data as "any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer IP address." These rights span our lives at home, at work, as consumers, as patients, in legal matters, and on the Internet.

The GDPR also contains provisions specific to children. The main purpose of this provision is on commercial internet services such as social networ king. If your organization collects children's personal data, you will need to have a system to verify children's ages; and have a process to obtain the consent of a child's parent or legal guardian.

While the GDPR is an essential step to strengthen EU citizens' fundamental rights in the digital age; it can also facilitate business by simplifying rules for organizations in the Digital Single Market. A single data privacy law will eliminate the current fragmentation and costly administrative burdens, leading to savings estimates of around €2.3 billion a year.

In the law enforcement and criminal justice sectors, the GDPR is designed to safeguard citizens' fundamental right to data protection whenever personal data is used by criminal law enforcement authorities. In particular, it will ensure that the personal data of victims, witnesses, and suspects of crimes are duly protected; and it will help cross-border cooperation in the fight against crime and terrorism.

To whom does it apply?

The GDPR applies to the collection of personal data of EU citiz ens anywhere in the world. Note, that GDPR compliance applies even if the data processor or data controller is outside the EU; they fall under the scope of the GDPR simply by processing EU citizen data. This includes organizations that provide cloud services to EU customers that are based outside the EU.

Because any organization that works with personal information relating to EU citizens will have to comply with the requirements, GDPR will become the first global data protection law. So the big question is, "how does this affect your cybersecurity strategy."

Cybersecurity as business driven security

The GDPR requires organizations to know exactly what, when, and where they are collecting information from covered persons, processing the information, storing the information (and how long), and sending information to others, including across borders. Moreover, all of this has to be sufficiently documented, the risks assessed, and appropriate technical and organizational measures implemented to bring residual risk within tolerable levels. Because of the required level of detailed documentation, it is unlikely that an organization can fulfill their obligations under the GDPR and de monstrate their compliance using spreadsheets and word processing documents. Compliance has to be independently verified so adequate and complete documentation will be critical to keeping audit costs down and audit and regulatory engagements and findings as short as possible.

In the process of an organization assessing their GDPR-related risk and determining the appropriate technical and organizational measure to treat the risk, organizations must understand the risk in business terms. Without translating technical risk into terms that senior business leaders can understand, it is difficult for the organization to make well-informed decisions about the allocation of scarce human and capital resources across the organization's risk portfolio. The application of a Business-Driven Security Strategy to GDPR will avoid this problem and promote better risk management practices of technical risk managers as well as business leaders.

What does GDPR mean for your GRC/business risk management strategy?

Business Risk Management / GRC tools play a critical role in helping organizations fulfill GDPR obligations.

- All GDPR-related infrastructure, business processes, policies and procedures, risks, controls, third parties, business resiliency plans, and outstanding issues and remediation plans must be documented.
- The level of GDPR-related risk must be assessed for every IT infrastructure element, business process, and third party where covered information is processed, stored, or transmitted. In assessing risk, consideration should be given to both electronic and physical security as well as to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to covered data.
- Documenting the implementation of appropriate technical and organizational measures to help ensure a level of security appropriate to the risk. Appropriate technical and organizational measures are to be designed to protect covered data against accidental or unlawful destruction or accidental loss and to prevent any unlawful forms of processing, in particular any unauthorized disclosure, dissemination or access or alteration of personal data.

Technical measures include technologies implemented to help protect and mediate physical and electronic access to your systems and data, detection tools to expose and respond to unauthorized access, etc. Organizational measures include policies and procedures around vetting new hires and third parties that handle or access covered data, data input and edit controls, data input and output file reconciliations, employee education and training around privacy, SDLC procedures incorporating information security assessments, third-party governance, business resiliency and the like.

- Documenting the results of periodic tests of technical and orga nizational measures to ensure that they continue to be designed and operating effectively. Testing may be performed manually or result from the implementation of automated continuous control monitoring.
- Monitoring the overall status of the GDPR risk profile. For most organizations, GDPR risk will not remain static. As the volume of covered data changes, the organization's products and processes change, and geographic footprint and third party dependencies change, so too will the organization's GDPR risk profile. As risk assessments and control testing are completed gaps in technical and organizational measures will be identified that must be remediated to comply with GDPR. By conso lidating all of your GDPR-related compliance information in one platform, not only are you able to readily demonstrate compliance with GDPR but you are informed as risk increases, changes in the organization occur that warrant attention, issues are exposed that must be actively monitored to remediated, and security incidents arise that must be actively managed and reported to authorities and the customers that may have be subject to the incident.

Above are the core elements necessary to transform a technical security approach to GDPR to one that is business driven. In addition, the following obligations imposed by GDPR can be documented with a configurable business risk management / GRC tool:

- Cataloguing and managing EU citizen inquiries about whether their data is being handled by the organization
- Steps taken to respond to EU citizen requests to be "forgotten"
- Managing exceptions to the explicit consent requirements of GDPR, including exceptions around the requirement to obtain parental consent for children under 16 years of age.

What does GDPR mean for your identity strategy?

RSA believes that Identity is the most consequential threat vector with 63% of confirmed breaches in 2015 resulting from compromised credentials 81% of hacking-related breaches leveraged either stolen and/or weak passwords (2017 Verizon Data Breach Investigations Report). This underscores the need for stronger authentication mechanisms that are convenient to the end user, while still secure and in compliance with corporate and regulatory policies. Building a strong Identity and Access Management (IAM) program is central to reducing identity risks that can be exploited by hackers to infiltrate and steal personal information.

An IAM solution can help solve three fundamental challenges for organizations to protect sensitive and personal information: are my users who they claim they are; do they have the right level of access; and is the access in compliance with policies? First, organizations need to provide convenient yet secure access in order for users to find the information the y need (regardless of whether the application is on premise or in the cloud) and deliver the confidence that people are who they say they are. Secondly, organizations need to ensure users have the appropriate level of access to do their jobs. This involves requesting, reviewing, granting, and revoking user access; using automated processes that enable business owners to make access decisions. Lastly, proving compliance is critical to showing regulators how organizations are complying with GDPR. With identity governance controls and reporting that connect back to corporate GRC policies, it is much easier and efficient to run reports to show continuous compliance aligned to the regulations. All three components provide visibility and control so that your organization can maintain continuous compliance.

Compromised accounts, stolen credentials, or mismanaged provisioning all could be seen as a weakness in GDPR compliance. Organizations need to show they are taking a proactive approach to managing access to personal information. In the event of a breach, comprehensive audits to prove a high level of access control will help strengthen the argument that the organization made a conscientious effort in line with GDPR guid ance to protect identities. As we know, the costs of non-compliance with GDPR are steep, up to 4% of annual global revenue or €20 Million (whichever is greater). Therefore securing your identities and access governance are imperative steps to help meet GDPR requirements.

What does this mean for your threat detection & response strategy?

Many organizations have deployed technical measures around data protection infrastructure, ranging from firewalls and spam filters, to Data Loss Prevention (DLP) solutions and Intrusion Prevention Systems (IPSs). Still, we hear about data breaches that affect millions of users.

Breaches continue because, as security infrastructure became standardized, threat actors have become adept at targeting attacks and evading defenses. The operating presumption must be that your organization's IT infrastructure is under continuous attack, and potentially already compromised in multiple ways. This shifts the conversation from threat prevention, to threat detection and response.

Organizations should consider technology solutions that provide visibility across the network utilizing data from logs, packets, endpoints, and threat intelligence to rapidly detect and understand the full scope of a compromise to aid in fast and effective response.

By using solutions with behavioral analysis and machine learning, organizations can correlate indicators and assigns risk scores that identify anomalies that warrant investigation. Unlike traditional prevention systems, this will help your organization hunt for the threats that have successfully invaded your organization. Undetected, such exploits can wreak havoc on your infrastructure and intellectual property, and can lead to the types of data breaches of EU citizen personal data that the GDPR specifically covers.

Another consideration, would be to adopt a solution that allows for configuration to limit exposure of privacy-sensitive metadata and raw content (packets and logs) using a combination of techniques, including:

- Data Obfuscation – Privacy-sensitive metakeys can be obfuscated for specified analysts/roles
- Data Retention Enforcement – Retain privacy-sensitive data only as long as needed
- Audit Logging – Audit trail for privacy-sensitive activities, e.g., attempts to view/modify data

Summary

Ultimately, the objective of the GDPR is to shield all EU citizens from privacy and data breaches in an increasingly connected and data-driven world. GDPR modernizes and expands the 1995 Data Protection Directive to drive uniformity around interpretation and implementation of data protection rules as well as territorial reach to include any organization, in any country that is a controller or processor of EU citizen personal data.

EU citizens are entitled to key personal data protection "rights' under GDPR:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure – also known as the right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object

A tiered approach to fines has been established by GDPR stretching from 2% of annual global revenue for not having their records in order, not informing the supervising authority and data subject (individual) about a breach or not conducting an impact assessment to up to 4% of annual global revenue or €20 Million (whichever is greater) for the most serious violations; e.g. not having sufficient customer consent to process data or violating core concepts. It is important to note that these rules apply to both controllers and processors -- meaning 'clouds' will not be exempt from GDPR enforcement. In other words, failure to comply could be debilitating for some organizations.

Business-driven security solutions from RSA

RSA is a leader in advanced cybersecurity solutions delivering Business-Driven SecurityTM so organizations of all sizes can take command of their evolving security posture in this uncertain, high-risk world.

Our solutions and services uniquely link business context with security incidents so organizations can reduce risk and be sure they are protecting what matters most.

More specifically, RSA is the ONLY company that enables the three most critical elements of a sound security strategy: rapid response and detection, control at the user access level, and business risk management.

The RSA® Archer® Suite is engineered to empower organizations to manage multiple dimensions of risk with solutions built on industry standards and best practices on one configurable, integrated software platform.

The RSA® SecurID® Suite is designed to enable organizations of all sizes to accelerate their business while minimizing identity risk and delivering convenient and secure access to the modern workforce. The RSA Secur ID Suite leverages risk analytics and context-based awareness designed to ensure the right individuals have the right access, from anywhere and any device.

The RSA® NetWitness® Platform is a threat detection and response platform that is designed to allow security teams to detect and understand the full scope of a compromise by leveraging logs, packets, endpoints, and threat intelligence. By aligning business context to security risks, RSA NetWitness Platform is engineered to provide the most advanced technology to analyze, prioritize, and investigate threats making security analysts more effective and efficient.

About RSA

RSA offers business-driven security solutions that uniquely link business context with security incidents to help organizations manage risk and protect what matters most. RSA solutions are designed to effectively detect and respond to advanced attacks; manage user identities and access; and, reduce business risk, fraud, and cybercrime. RSA protects millions of users around the world and helps more than 90% of the Fortune 500 companies thrive in an uncertain, high-risk world.
For more information, go to **rsa.com**.