Secureworks®

WHITE PAPER

How GDPR Affects Your Security Strategy

Integrating GDPR Compliance into a Holistic Security Posture for your organization

The General Data Protection Regulation[1] is a European Union regulation with the full title of 'Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, which repeals Directive 95/46/EC (General Data Protection Regulation)'.

It was the first comprehensive overhaul and replacement of European data protection legislation in over twenty years, and is a landmark regulatory framework on par with Sarbanes-Oxley in 2002. It has effectively replaced the varying implementations across Europe of the earlier EU Data Protection Directive with a single harmonized EU regulation. As a result, organizations today have a standardized set of expectations about how they must manage and protect personally identifiable information on employees, clients and other applicable data subjects.

With the right approach and help, organizations can use the requirements laid down by GDPR that affect information security to promote privacy, security, and business enablement.

Any organization that holds data on EU citizens, regardless of where it is domiciled — within the EU or otherwise — is in scope. Likewise, organizations processing data within the EU on any data subject, regardless of the data subject's location, may be in scope.

How does GDPR affect your security approach?

GDPR provides a comprehensive data protection regime, of which data security is one part. Privacy and data protection issues have far-reaching implications for many aspects of business operations and GDPR requires significant changes across many parts of the organization. As regulators and innovators trade blows in this era of rapid technological change, take this unique opportunity to initiate dialogue within your organization about proactive security culture, increased visibility and data protection strategies.

While data security is by no means the only consideration, it is a necessary one. Indeed, GDPR explicitly calls for 'appropriate security' to help achieve the objectives of the Regulation.

The fundamental objectives of GDPR are clearly laid out in Article 5 'Principles relating to processing of personal data'.

These state that personal data must be:

- processed lawfully, fairly and in a transparent manner
- collected and processed for specific, explicit and lawful purposes only
- kept to the minimum required for the purpose

[1] General Data Protection Regulation, http://ec.europa.eu/justice/data-protection/ reform/files/regulation_oj_en.pdf

- must be accurate and current stored in a way that allows identification of the data subject for no longer than is needed for its purpose
- processed in a manner that ensures appropriate security of the personal data.

What is appropriate security?

Again, Article 5 is explicit about the objectives – the data must be protected against unauthorized or unlawful processing. It must be also be protected against accidental loss, destruction or damage.

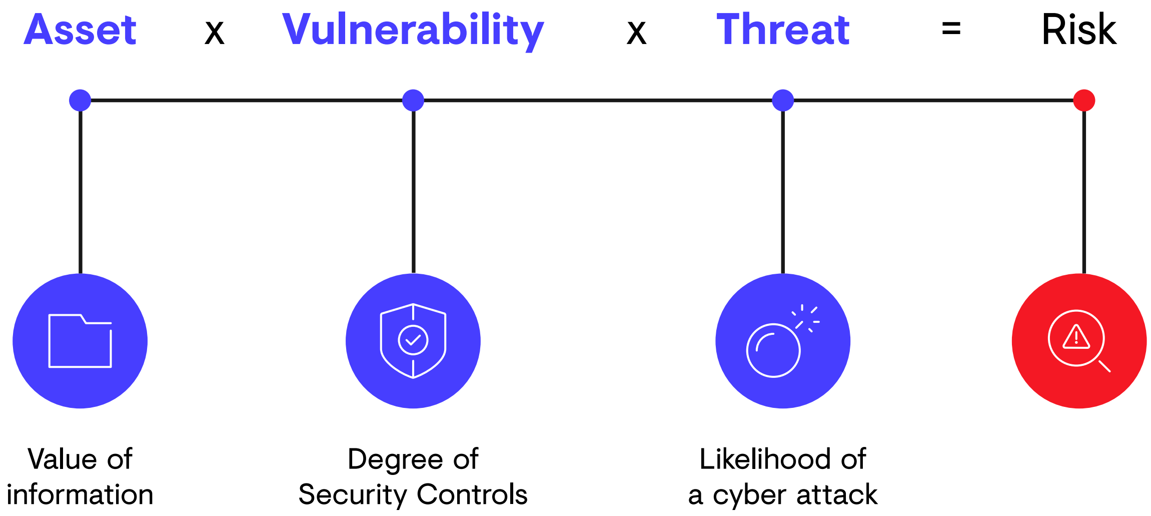

Figure 1: Security Risk Formula

However, rather than offering a checklist of specific controls, GDPR differs from many other compliance frameworks in that it requires organizations to implement control 'to ensure a level of security appropriate to the risk'. This implies taking a risk-based view of security[2], and following a risk-based program and framework (Figure 1). While this is an approach that has gained increasing currency, for some organizations it may require a dramatic shift in how they tackle security.

Understanding risk-based security

Risk-based security means establishing priorities and making decisions through evaluating data sensitivity, system vulnerability and the likelihood of threats. However, it demands more than simply factoring risk into deploying security solutions. It's an entire holistic approach, building an understanding of risk into every security related decision.

[2] https://www.secureworks.com/blog/cybersecurity-risk-questions-boards-should-be-asking

Ultimately, a mature information security posture is built around an organization's understanding of risk in the context of the needs of the business. This risk-based security approach should be used to objectively identify what security controls to apply, where they should be applied and when they should be applied.

GDPR as an opportunity for business enablement

There are multiple further requirements within GDPR concerning data management that require a fresh approach, such as Privacy by Design and Default. To maneuver towards GDPR compliance, organizations should anticipate using a lot of business resources, time and attention, both within the security function and more widely throughout the organization.

However, GDPR is a great opportunity to promote a strong security agenda, based on a pragmatic, holistic, risk-based approach that works in both the short and long term to create business enablement as well as regulatory compliance.

After all, security threats impact the organization's brand perception and brand value worldwide. They affect its financial value – share values may plunge in the storm of publicity surrounding a data breach[3]. They threaten its digital capital, its IP, its financial assets and its data. Clearly an organization dealing with the aftermath of a major breach is not one with its attention entirely focused on its business goals.

As a result, addressing the security requirements of GDPR comprehensively will not just ensure that organizations avoid penalties and protect customer and stakeholder privacy, but will also help establish a valuable competitive advantage and build trust with their clients, end users and other stakeholders.

What does strong GDPR-appropriate data security include?

There's more to security than just prevention. In fact, a strong security posture recognizes that prevention is not possible 100% of the time. Responding to GDPR or any similar regulatory requirement by simply buying more preventative technology is a mistake because it is not part of a larger strategy.

Instead, there are three critical components to a strong security approach: protection, detection, and response. These form not just the backbone of an initial GDPR-focused security program, but must become internalized until they are ingrained within the muscle memory of an organization, becoming the very core of its security operations.

Effective protection

Effective protection is based on pragmatic, risk-based, foundational security controls, involving technology, people, process and data and other assets. It requires an

Risk-based security is:

- Contextualized to business strategy
- Pragmatic
- Business impact driven, not just compliance driven
- Based on the recognition that you will be compromised
- People, process and technology based
- Sees technology as a tool, not a goal
- A permanent approach, not a short term fix

[3] TalkTalk share price plunges twice as deep..., November 13 2015, http://www.cityam. com/228714/talktalk-share-price-plunges- twice-as-deep-as-sony-carphone-warehouse-barclays-and-ebay-after-cyber-attacks

understanding of your responsibilities and of what you are protecting that comes from thoroughly knowing your business-critical data and assets and being aware of who has access rights to them and how secure their practices are. Effective protection combines the assessment of possible threats through advanced threat intelligence, and a risk- based approach to protecting those assets and associated processes.

It requires 24x7 monitoring capabilities that go beyond simply flagging threats to the ability to access extensive intelligence on threat actors and their tradecraft. It needs the capability to query and analyze intrusion data.

Successful detection

Successful detection requires enhanced visibility across the entire enterprise, network, endpoints, mobile, cloud, software as a service and more. GDPR requires the ability to detect breaches - if you don't have visibility, you can't monitor, and you won't be able to detect.

That lets you accelerate and hone your response by pinpointing exactly which systems are compromised, which data has been accessed, how it happened and how you can repair and restore them. It lets you judge whether a breach that is reportable under GDPR has occurred and which data it affects or whether you have caught the intrusion in time to prevent data in scope being compromised. The more precisely you can detect, the more granular and efficient your response can be.

Timely incident response

Timely incident response requires preparation above all– knowing and documenting your organizational risks in advance, allocating roles including responsibility for decision making, understanding statutory reporting requirements (including deadlines and formats), planning how to mitigate impact on the business, being ready to inform stakeholders and more. All these aspects need to be thoroughly tested and participants trained. GDPR requires notification to the regulator within 72 hours of breach discovery, meaning there is no time available to reinvent the wheel and no time to find that your incident response plans don't work.

Of course, reporting is just the first piece of incident response. You must contain any breaches, remediate compromised systems and examine the entire security breakdown to learn from the incident and prevent it from happening again.

All of these aspects must be underpinned by comprehensive policies and procedures, taking care to improve governance and business engagement by assigning accountability and ensuring that users understand their security responsibilities through appropriate training.

Conclusion: Compliance and beyond

GDPR poses different challenges to each organization. Understanding and acting on the implications for your own organization is vital. That means taking a risk-based approach to ensure that you are doing what you need to do to manage your own specific risks to personal information.

While virtually all organizations are implementing changes to become GDPR compliant, some have taken partial advantage of existing compliance to other security mandates and frameworks, such as ISO 27001 and PCI by extending those measures to protection of personal data. Even so, further work is required to comply with the security, reporting and data protection benchmarks of GDPR.

For others, without any prior preparation, GDPR is a challenge with a lot at stake. Working with a trusted security partner on the information security and incident response parts of the puzzle can really help make that challenge less daunting and the deadlines less resource crippling.

Because GDPR is not prescriptive about means, calling instead for appropriate technical or organizational methods depending on the risk profile, access to a portfolio of expert GDPR services makes sense. Rather than buying off-the-shelf GDPR solutions, take a risk-based approach; obtain the support that you need, be it an assessment of your current GDPR maturity, gap remediation and GDPR program development, Data Protection Risk Assessments, program implementation, testing or incident response.

Irrespective of the asset, a risk driven approach to security is highly beneficial. The end result will be security operations, based on protection, detection and response that increase your security posture, not just for GDPR but for business enablement in general.

For more information, or to speak with a security specialist, call the regional numbers located on the back page.

GDPR isn't optional, but it presents an opportunity to review security programs and develop a risk-based approach. Ultimately, its risk-based approach can be extended to any information that is of value to the organization, be it intellectual property, personally identifiable information, or any other core data.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a global cybersecurity leader that protects customer progress with Secureworks® Taegis™, a cloud-native security analytics platform built on 20+ years of real-world threat intelligence and research, improving customers' ability to detect advanced threats, streamline and collaborate on investigations, and automate the right actions.

Corporate Headquarters

United States
1 Concourse Pkwy NE #500
Atlanta, GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp