



THE GENERAL DATA PROTECTION REGULATION (GDPR) PRIMER

*What The Insurance Industry Needs To Know, And
How To Overcome Cyber Risk Liability As A Result.*

By: Rob Vazquez

TABLE OF CONTENTS

TABLE OF CONTENTS.....	2
Author page.....	3
ROB VAZQUEZ , M.B.A., M.S.	3
What is the General Data Protection Regulation (GDPR)?	5
Scope	6
Single set of rules and one-stop shop	6
Responsibility and Accountability	6
Consent for Adults and Children.....	8
Data Protection Officer (DPO)	8
Pseudonymizing.....	8
Data Breaches	8
Sanctions and Enforcement	9
Right to Erasure.....	9
Data Portability.....	9
Data Protection by Design and by Default.....	10
Records of Processing Activities.....	10
Applicability and Impact (Comparison of US Compliance and GDPR).....	11
Systems Perspective and SME's.....	11
At the root of system breaches	13
The Fox chasing the Hound	13
Credit Scores and Assessments	14
Changing Attack Surface	15
Cyber Insurance Industry Continues to Expand	16
Key Figures for Comparison	16
How to insure a client in the EU after GDPR?	17
GDPR focused controls assessment review.....	17
Data Breach Prevention based cyber security posture.....	18
Recommended Technical Solutions for GDPR Compliance	19
Solution (GDPR in a Box)	19
Securing Personal Data	21
Data Breach Prevention	21
Data Breach Notification (GDPR).....	22
Summary.....	23

AUTHOR PAGE

ROB VAZQUEZ , M.B.A., M.S.

President and Chief Security Officer at Clarium Managed Services. Leader in global information systems, pioneer in cyber-security, industry expert, speaker, and consultant. Rob has assisted businesses in their global networking and in ensuring their IT security is watertight against a constantly evolving 'attack surface'.

Throughout his 30 years' experience involving the structuring and deployment of large-scale IT projects, security and compliance have always been a concern of his and featured in all his projects worldwide. Rob has led global projects – including the design and implementation of the largest encrypted IP based network in the Southern Hemisphere in 2000 with France Telecom – the first of its kind.

As President and Chief Security Officer of Clarium Managed Services, he has led the company's growth inside local and global markets. The firm is now a Managed Service Provider to most of the enterprise technology manufacturers, including Palo Alto Networks.

Rob holds an M.B.A with concentration on Information Systems from Nova Southeastern University, as well as a separate Master's of Science in Dispute Resolution (Arbitration), also from Nova. During his career, he has attained over (30) top technical certifications from most of the leading technology manufacturers. He sits on various industry and agency committees to promote a safe cyber world.

THE EU GDPR UNVEILED IN 1 MINUTE

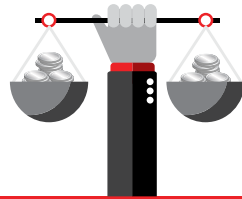
The primary objective of the GDPR is to transfer controls to citizens and residents over their personal data and vastly simplify the regulatory environment for international businesses by unifying data regulations within the EU.

Here is what it means to your business:

Strict Sanctions:

finances can be levied up to

4% of annual worldwide revenue or



€20 million whichever is the greater.

GDPR is far reaching and applies to entities that process personal data **even if they are not based in the EU.**



Data transferred outside the **EU** will still be protected under the **GDPR.**

Affirmative Consent:

must be clear and understood by data subject before the processing of personal data.



The right to be forgotten: is broadened and includes permanent erasure of records.

Processing of **personal data of children** under the age of 16 without parental consent is forbidden.



WITHIN **72 hours** of a data breach controllers must report the breach and all subsequent information



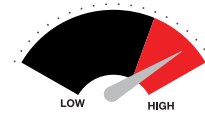
A Data Protection Officer (DPO):



must be retained by entities that process a high volume of personal data, and as a form of best practice.

Many certifications such as **ISO 27001 or CISSP** will contribute to the demonstration of **"adequate technical and organizational measures"** to protect personal data.

Where the risk is high for privacy breach: assessments must be carried out to manage such risk.



Foreign entities will benefit from **One-stop shop** compliance instead of multiple Nation States.

WHAT IS THE GENERAL DATA PROTECTION REGULATION (GDPR)?

The General Data Protection Regulation (GDPR) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to transfer controls to citizens and residents over their personal data, and to vastly simplify the regulatory environment for international business by unifying the regulation within the EU. When the GDPR takes effect, it will replace the Data Protection Directive from 1995. The regulation was adopted on April 27, 2016. It becomes enforceable from May 25th, 2018 after a two-year transition period and, unlike a directive, it does not require any triggering legislation to be passed by member states and is thus directly binding and applicable.

The changes which are to be ushered in by the GDPR from

Friday May 25th, 2018 are substantial and ambitious. The Regulation is one of the widest ranging pieces of legislation passed by the EU in recent years, and concepts to be introduced such as the 'right to be forgotten', data portability, data breach notification and accountability (to call out only a few) will take some getting used to. Even its legal medium - a regulation not a directive - makes the GDPR an unusual piece of legislation for data protection lawyers to analyze. Even more paramount is how these regulations will impact the assessing, writing, and implementation of data protection "Cyber" insurance products throughout the European Union. Concerns and risk factors are considered as well for North American entities that hold agency in the EU, and process data within the EU, regardless of their central office.

The proposal for the European Data Protection Regulation contains the following key requirements:

SCOPE

The regulation applies if the data controller (organization that collects data from EU residents) or processor (organization that processes data on behalf of data controller e.g. cloud service providers) or the data subject (person) is based in the EU. Furthermore, the Regulation also applies to organizations based outside the European Union if they collect or process personal data of EU residents. Per the European Commission, “personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address.” The regulation does not apply to the processing of personal data for national security activities or law enforcement; however, the data protection reform package includes a separate Data Protection Directive for the police and criminal justice sector that provides robust rules on personal data exchanges at national, European and international level.

SINGLE SET OF RULES AND ONE-STOP SHOP

A single set of rules will apply to all EU member states. Each member state will establish an independent Supervisory Authority (SA) to hear and investigate complaints, sanction administrative breaches, etc. SA’s in each member state will cooperate with other SA’s, providing mutual assistance and organizing joint operations. Where a business has multiple establishments in the EU, it will have a single SA as its “lead authority”, based on the location of its “main establishment” (i.e., the place where the main processing activities take place). The lead authority will act as a “one-stop shop” to supervise all the processing activities of that business throughout the EU. A European Data Protection Board (EDPB) will coordinate the SAs.

There are exceptions for data processed in an employment context and data processed for the purposes of national

security, that still might be subject to individual country regulations.

RESPONSIBILITY AND ACCOUNTABILITY

The notice requirements remain and are expanded. They must include the retention time for personal data and contact information for data controller and data protection officer must be provided.

Automated individual decision-making, including profiling (Article 22) is made disputable. Citizens now have the right to question and fight decisions that affect them that have been made on a purely computer generated basis.

To be able to demonstrate compliance with the GDPR, the data controller should implement measures which meet the principles of data protection by design and data protection by default. Privacy by Design and by Default require that data protection measures are designed into the development of business processes for products and services. Such measures include pseudonymizing personal data, by the controller, as soon as possible.

It is the responsibility and liability of the data controller to implement effective measures and can demonstrate the compliance of processing activities even if the processing is carried out by a data processor on behalf of the controller.

Data Protection Impact Assessments must be conducted when specific risks occur to the rights and freedoms of data subjects. Risk assessment and mitigation is required and prior approval of the Data Protection Authorities (DPA) is required for high risks. Data Protection Officers are to ensure compliance within organizations.

They must be appointed:

- < **for all public authorities, except for courts acting in their judicial capacity**
- < **if the core activities of the controller or the processor consist of**
- < **processing operations which,**

```
extern double StopLoss =200; // SL for an opened order
extern double TakeProfit =39; // TP for an opened order
extern int Period_MA_1=11; // Period of MA 1
extern int Period_MA_2=31; // Period of MA 2
extern double Rastvor =28.0; // Distance between MAs
extern double Lots =0.1; // Strictly set amount of lots
extern double Prots =0.07; // Percent of free margin
```

```
Refresh rates
Minimal number
Free margin
Price of 1 lot
Step is changed
(Symb,MODE_MINLOT);
eMargin();
(Symb,MODE_MARGINREQUIRED);
(Symb,MODE_LOTSTEP);
```

```
extern double Stoploss =200; // SL for an opened order
extern double TakeProfit =39; // TP for an opened order
extern int Period_MA_1=11; // Period of MA 1
extern int Period_MA_2=31; // Period of MA 2
extern double Rastvor =28.0; // Distance between MAs
extern double Lots =0.1; // Strictly set amount of lots
extern double Prots =0.07; // Percent of free margin
```

by their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale

- < **processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10**

CONSENT FOR ADULTS AND CHILDREN

Valid consent must be explicit for data collected and the purposes the particular protected data is used for. Consent for children must be given by the child's parent or custodian, and verifiable. Data controllers must be able to prove consent, and consent can be revoked without cause.

DATA PROTECTION OFFICER (DPO)

A Data Protection Officer is assigned when data processing is carried out by a public jurisdiction or judicial authority, or in the private sector where processing is carried out by a controller whose core activities consist of processing operations that require regular and systemic monitoring of the data subjects. This person must possess expert level knowledge of data protection laws and practices and will assist the controller or processor in monitoring the internal compliance with GDPR.

The DPO is similar but not the same as a Compliance Officer as they are also expected to be proficient at managing IT processes, data security (including dealing with cyber-attacks) and other critical business continuity issues around the storage and processing of personal and sensitive data. An equivalent role in North America would be a Chief Information Security Officer, or CISO. The skill set required stretches beyond understanding legal compliance with data protection laws and regulations. The appointment of a DPO within a large organization

will be a challenge for business as well as for the individual concerned. There are a myriad of governance and human factor issues that organizations and companies will need to address given the scope and nature of the appointment. In addition, the DPO will need to create their own support team and will also be responsible for their own continuing professional development as they need to be independent of the organization that employs them, effectively as a "mini-regulator".

PSEUDONYMIZING

Pseudonymizing is a process that transforms personal data in such a way that the resulting data cannot be attributed to a specific data subject without the use of additional information. It is one of the key recommendations of Article 32, "Security of Processing".

An example of pseudonymizing is encryption, which renders the original data unintelligible and the process cannot be reversed without access to the correct decryption key. The GDPR requires that this additional information (such as the decryption key) be kept separately from the pseudonymized data. Pseudonymizing is recommended to reduce the risks to the concerned data subjects, and also help controllers and processors to meet their data protection obligations.

Although the GDPR encourages the use of pseudonymizing to "reduce risks to the data subjects," pseudonymized data is still considered personal data and therefore remains covered by the GDPR. Lastly, pseudonymizing data is encouraged by the GDPR, not *mandated*. This is an important distinction in later discussions around applicability and impact.

DATA BREACHES

Under the GDPR, the Data Controller will be under a legal obligation to notify the Supervisory Authority (SA) without unreasonable delay. The reporting of a data breach is not subject to any *de minimis* standard and must be reported to the Supervisory Authority (SA) within 72 hours of the data breach.

Individuals must be notified if adverse impact is determined. In addition, the data processor must notify the controller without undue delay after becoming aware of a personal data breach.

However, the data processor or controller do not have to notify the data subjects if anonymized data is breached. Specifically, the notice to data subjects is not required if the data controller has implemented pseudonymizing techniques like encryption along with adequate technical and organizational protection measures to the personal data affected by the data breach.

SANCTIONS AND ENFORCEMENT

The primary objective of GDPR is to implement a consistent set of regulations that enforce data protections uniformly across The European Union. They are by far the most aggressive set of regulations ever imposed on a set of nation states; and certainly leave little doubt as to the intent.

Some of the biggest differences between GDPR, its predecessor The Data Protection Directive, and other major industry compliances are as follow:

- ◆ **Penalty. The penalties for noncompliance are daunting. Ranging on occurrence and severity of the infraction the penalty can be:**
 - < **A warning in writing in cases of first and non-intentional non-compliance**
 - < **Regular periodic data protection audits**
 - < **\$10m € or 2% of annual worldwide turnover, whichever is greater**
 - < **\$20m € or 4% of annual worldwide turnover, whichever is greater**
- ◆ **Depth and breadth of compliance. GDPR goes far deeper than any compliance as well regarding its classification of personally identifiable information (PII). If you**

compare GDPR to the Health Care Portability Act (HIPAA) in the United States, GDPR includes areas such as biometrics and/or DNA. Pieces of data not currently legislated in other regulations. If the subject data can somehow lead to the identification of a natural person it is protected under GDPR. The new identifiers include:

- < **Genetic**
- < **Mental**
- < **Cultural**
- < **Economic**
- < **Social Identity**

Immediately this makes one wonder how some of the major multinational companies that deal with this data will circumnavigate GDPR? Take for example a popular website to track ancestry such as ancestry.com. In the strict interpretation of GDPR that entity cannot transact in the EU. If the subject matter of its data collections are protected individuals in the EU, who can subsequently be identified. From a purely information systems viewpoint this is an insurmountable task to try to organize compliance while not disrupting the normal business operation of an information system or a business in general.

RIGHT TO ERASURE

A right to be forgotten was replaced by a more limited right to erasure in the version of the GDPR adopted by the European Parliament in March 2014. Article 17 provides that the data subject have the right to request erasure of personal data related to them on any one of several grounds including non-compliance with article 6.1. This includes a case where the interests or fundamental rights override the legitimate interests of the controller and freedoms of the data subject which require protection of personal data.

DATA PORTABILITY

A person shall be able to transfer their personal data from one electronic



processing system to and into another, without being prevented from doing so by the data controller. In addition, the controller in a structured and commonly used open standard electronic format must provide the data. The right to data portability is provided by Article 20 of the GDPR. Legal experts see in the final version of this measure as a new right created that reaches beyond the scope of data portability between two controllers as stipulated in Article 18.

DATA PROTECTION BY DESIGN AND BY DEFAULT

Data protection by Design and by Default requires that data protection be designed into the development of business processes for products and services. This requires that privacy settings must be set at a high level by default, and that technical and procedural measures should be taken care by the controller to make sure that the processing, throughout the whole processing lifecycle, complies with the regulation. Controllers should also implement mechanisms to ensure that personal data is only processed when necessary for each specific purpose.

A report by ENISA (the European Union Agency for Network and Information Security) elaborates on what needs to be done to achieve privacy and data protection by default. It specifies that encryption and decryption operations must be carried out locally, not by remote service, because both keys and data must remain in the power of the data owner if any privacy is to be achieved. The report specifies that outsourced data storage on remote clouds is practical and relatively safe, as long as only the data owner, not the cloud service, holds the decryption keys.

RECORDS OF PROCESSING ACTIVITIES

Records of processing activities must be maintained, that include purposes of the processing, categories involved and envisaged time limits. These records must be made available to the supervisory authority on request.

APPLICABILITY AND IMPACT (COMPARISON OF US COMPLIANCE AND GDPR)

SYSTEMS PERSPECTIVE AND SME'S

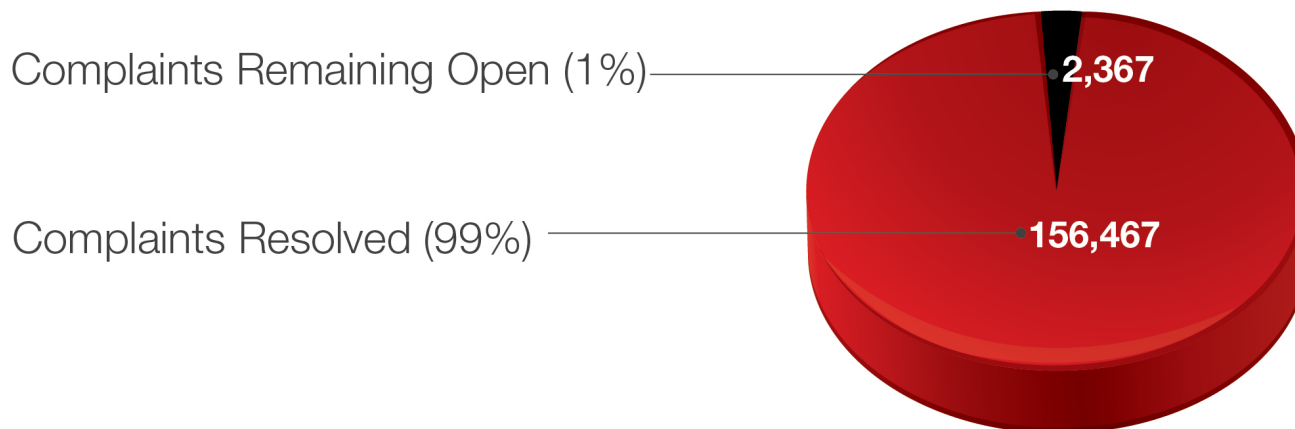
In reviewing applicability there is a wealth of history in the United States dating back to the early 1990's that can be used as historical reference. Particularly in light of the Health Insurance Portability and Accountability Act of 1996, which was further enhanced by the HITECH regulations of 2013. Collectively, HIPAA/HITECH provide one of the most stringent compliance regulations to date. It is a very relevant body of rules to compare to GDPR because of the magnitude of penalty and coverage it provides on the day-to-day business of even a small physicians practice.

At the core of GDPR is the applicability on Small to Medium Enterprises (SME's) from a systems perspective. Let's face it, most small business do not utilize advanced security devices and protocols. Typically, these safeguards are employed by large enterprise entities that can both afford the tremendous cost of procurement, and secure the human resource talent to implement such tactics. Moreover, many SMEs do not understand or realize the importance of data security. 82% of them believe that they are not a target for cyber-attacks, as they do not have anything worth stealing. This contains two significant fallacies:

1. **Laissez faire stance (it will not happen to me).** According to the Kaiser Family Foundation there are currently over 925,000 active physicians in the United States. All of which fall under the privacy act for protected patient data (HIPAA/HITECH). HIPAA is the most robust compliance regulation to compare to GDPR. An estimated 78% of these physicians do not comply with HIPAA, or take the enforcement of HIPAA as something that will not happen to them. This attitude is driven by the low percentage of enforcement since enactment, and of course cost to properly secure Electronic Patient Health Information (ePHI). Some interesting numbers to consider:

Status of All Complaints

April 14, 2003 - June 2017



Total Complaints Received 158,834

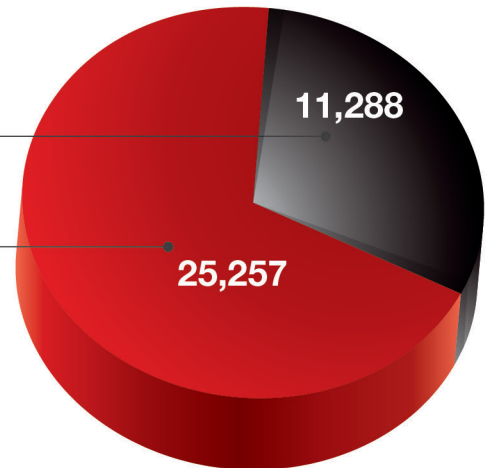
Since enactment of HIPAA on April of 2003 through June of 2017, only 158,000 privacy complaints have been received by Office of Civil Rights (OCR).

Total Investigated Resolutions

April 14, 2003 - June 2017

Corrective Action Obtained
(Change Achieved) (69%)

No Violation (31%)



Total Complaints Investigated 36,545

Of the 158,000 complaints received only 36,000 have been investigated with an even smaller amount submitted for Corrective Action (CA).

With such a small amount of complaints and enforcement, it is not difficult to see why medical practitioners in the United States take a *Laissez faire* position when it comes to the protection of patient data (ePHI). The key difference in comparing HIPAA enforcement to GDPR is that OCR does not actively audit practitioners without a preceding event to trigger the audit. Additionally, corrective action in many cases involves warnings and corrective counseling on enhanced methods to secure ePHI.

Clearly proactive and early enforcement of GDPR, and an infrastructure to support a myriad of uncompliant entities will drive the overall perception by an SME, and whether they should take the regulations seriously. Otherwise, GDPR will carry on much like HIPAA, a body of regulations that sound good, but in reality, are not being enforced. The legislators that formulated GDPR must have considered this because the adoption of Data Protection Authorities (DPA's) and Data Protection Officers (DPO's) is clearly aimed at proactive enforcement. Therefore, SMB's who take a *laissez faire* attitude on enforcement will be making a critical error.

2. **"I don't have anything worth stealing".** A recent shift in data breach has seen a rise in tactics that are aimed at stealing, or encrypting data for a ransom. Bad actors that are conducting these wide scale attacks are demanding a ransom small enough that the victim will not utilize their cyber insurance policy, since the ransom falls below the deductible of the policy. In May 2017, the standard ransom in the WannaCry attack was \$300 USD per device.

Several issues must be clarified. In many cases, the ransomware victim did not receive the decryption key from the attacker. This led to the destruction or permanent loss of data by the victim. Industry figures from just about any source now state that 60% of businesses that suffer a significant data breach go

“
I don't have anything worth stealing
”

out of business within (6) months. Additionally, combating one of the more popular responses as to why small businesses don't allocate budget to risk mitigation was that they, "feel they don't store any valuable data." Yet a good number reported that they in fact store pieces of customer information that are of significant value to cyber criminals:

- < **68 percent store email addresses**
- < **64 percent store phone numbers**
- < **54 percent store billing addresses**

We can clearly summarize that the above information not only constitutes a dangerous landscape for SME's in the EU, but insurers as well. The Federal Bureau of Investigation (FBI) estimates Ransomware to be a \$1 billion USD industry per annum. Irrespective of the financial losses, SME's are also placing themselves at risk for harsh enforcement penalties by GDPR.

The European Parliament reports that Micro, small and medium-sized enterprises (SMEs) constitute 99% of companies in the EU. They provide two thirds of private sector jobs and contribute to more than half of the total benefit created by businesses in the EU. Nine out of ten SMEs are actually micro enterprises with fewer than 10 employees. Therefore, the focus of any discussion on GDPR impact should start and end with SME's.

AT THE ROOT OF SYSTEM BREACHES

Human error and endpoint vulnerabilities now account for 90% of data breaches. Conventional anti-virus systems on computers, tablets, and smartphones have an effective stop rate of 37.6%. This movement from the edge of the network (firewall), to the endpoint has been driven by:

- ◆ **The advent of "smart firewalls" or next generation firewalls and routers that conduct a more**

thorough analysis of the activity in and out of the business and whether that activity is benign.

- ◆ **The propagation of software or zero day exploits that allow an attacker to bundle a piece of malware (such as ransomware) with an engineered attack like email phishing campaigns.**
- ◆ **The advent of digital currencies that allow an attacker to build untraceable payment methods into the complete attack package.**
- ◆ **Employees and contractors having devices that are used in the public space (off-net) and on the corporate network.**
- ◆ **Social Media and Social Engineering, finding insider information on anyone, from a factory employee, to their CEO is a simple task now with social media. Once the attacker has all the information required they could easily act like the victim's business colleague.**

Collectively, this attack type at the endpoint provides maximum value to any attacker; and has moved to the top as most utilized attack form.

THE FOX CHASING THE HOUND

Cyber insurance companies may have placed a significant amount of trust in conventional security measures in their overall underwriting process. Many have formed "alliances" or collaborations with security products and service providers based solely on brand, or past product performance. While this is a good form to slightly reduce the inherent risk of the policy in general $\leq 30\%$, most of these products and services are outdated, contain vulnerabilities which are well understood in the "dark web", or simply just do not work in the constantly evolving attack surface.

Black Hat 2017 was held this year in Las Vegas and featured some of the premier security manufactures in the industry. One in particular was a high-level sponsor of the show and likely spent



Human error and endpoint vulnerabilities now account for 90% of data breaches.



hundreds of thousands of USD to fund their sponsorship, and new security product demonstrations. After the show concluded on July 27th, 2017 just down the street at Ceaser's Palace another show was getting underway, Defcon 2017. The premier hackers convention held once a year in Las Vegas, Nevada.

Defcon dedicated two breakout sessions specifically on how to breach the product that days earlier was gleefully displayed by the security manufacturer at Black Hat. In total, (5) key vulnerabilities were demonstrated during those sessions. All of which would render the product ineffective at stopping a modern-day breach.

The fundamental problem here is not that these products are so vulnerable. It is that the entity in question is a well-respected multinational security manufacturer whom you would expect to be significantly ahead of the attackers, and their tactics. Insurance companies may place entirely too much faith on the brand of the security solution, or the past efficacy of the products they represent. This will be a significant mistake moving forward as insurance companies consider new collaborations to address potential risk from compliance mandates like GDPR.

Hackers view many of the mechanisms in place as outdated and in some cases comical. Much like many college textbooks represent a view that may have been relevant when written, the cybercrime industry moves at such a tremendous rate, sometimes daily, it is a losing battle for these security companies.

CREDIT SCORES AND ASSESSMENTS

The latest "advancement" in risk assessment are all the credit scoring entities flocking to the security market with an assessment that compiles some preset generic controls in a questionnaire, with an electronic sweep of the dark web to see if that company's assets are being sold or compromised. The entire result is than submitted to a "scoring" algorithm that provides insurance companies with a score they

can use to decide to underwrite cyber liability cover, or not.

These credit scores are as effective as taking an aspirin for a migraine headache. They may cover a few of the industry accepted controls, but without a significant review of internal controls and security mechanisms, they aren't worth the paper they are printed on.

There are legitimate and meaningful assessment organizations that will come to a customer's location and review all the controls and mechanisms. Unfortunately for the 99% of SME's in the EU, the cost will be too significant to the customer and may deter them from procuring a cyber liability policy that warrant's this level of review in the first place.

Many security solution providers like Clarium Managed Services are working on effective assessment and scoring platforms that will provide a meaningful result that insurance companies may rely on. In the case of Clarium, their GDPR specific assessment tool Assess+ will be available in November 2018 at a modest price point that can be absorbed by the entire insurance underwriting and solution procurement process.

CHANGING ATTACK SURFACE

As previously discussed, the primary areas of focus for an attacker is the endpoint. Many reasons follow as to why, but an insurance underwriter must place significant focus on how the potential insured is preventing breach at the endpoint (including point of sale systems) and smart devices that connect to the corporate network.

The attack surface has moved almost entirely to this corner of the attack plane and it is only going to get worse, and more focused.

An arsenal of new, portable and remotely accessible products are rapidly being introduced to the dark web, or hacking world. Tools that are "next generation" in their sophistication. Take for example the **LAN Turtle 3G**, a covert Systems Administration and Penetration Testing tool that provides stealth remote access

over cellular lines, network intelligence gathering, and man-in-the-middle monitoring capabilities. Housed within a generic "USB Ethernet Adapter" case, the LAN Turtle's covert appearance allows it to blend into many IT environments and provide direct "off-net" communication with the hacker.

If you take this same tool and imagine plugging it into an unsuspecting Point of Sale (POS) terminal at your favorite multinational coffee shop, with the perfected payload of sending back credit card swipes to the attacker, you can conclude how dangerous these next wave of tools are. Particularly at capturing not just financial information, but also critical personal or data subject information. Imagine a rewards or VIP program that same POS system may be linked to that contains many components of (PII). Quickly the next generation attack type comes together.

Over 90% of existing technologies, including 100% of conventional anti-virus manufacturers cannot stop this attack type. It requires a protection for exploit based attacks with injection stopping algorithms. A lot of words to digest, but in summary it means the assault on the endpoint is here to stay and should be the primary focus of a successful breach deterrent.



Tools that are "next generation" in their sophistication.

CYBER INSURANCE INDUSTRY CONTINUES TO EXPAND

KEY FIGURES FOR COMPARISON

A recent survey conducted by Forrester research (2017) illustrates some interesting comparisons with the US and the EU regarding Cyber insurance products.

EU By the numbers:

- ◆ More than one quarter (28%) of firms surveyed say they are planning to acquire some form of cyber cover in the next year.
- ◆ This is in addition to the nearly 40% that claim they already have some form of cyber cover.

US and EU

- ◆ 55% of respondents in the US say they have cyber cover already.
- ◆ 36% of respondents in the UK say they have cyber cover already.
- ◆ 30% of respondents in Germany say they have cyber cover already.

An interesting point here is that most US entities did not consider cyber related policies as important until a series of legislation in 2003 prompted mandatory notification for data breaches. Legislation, along with a significant series of successful attacks across the US led to aggressive uptake of the various cyber liability products.

This of course should track the same in the EU post GDPR with one of the signature components of GDPR being the mandatory breach notification. Something completely lacking or unenforceable in previous regulations across the EU.



HOW TO INSURE A CLIENT IN THE EU AFTER GDPR?

As businesses continue to flock to insurance companies at unprecedented rates, there are some key takeaways that any responsible cyber underwriter should consider prior to offering a cover; particularly in the EU. Fitch reports that cyber policies hit a staggering \$1.35 billion in 2016, and this information was collected prior to the cyber related attacks of WannaCry and Petya in 2017.

Additional industry figures also show Cyber policies increasing at over 300%, while some show the entire Cyber insurance market at \$20 billion USD by 2020. The numbers will continue to climb, and in the case of the European Union, they will see triple digit increases in the next (5) years as insureds will attempt to transfer risk for GDPR, *with insurance policies*.

GDPR will require incredible investments by companies to improve not just their technology, but also their processes and controls. Concluding that this will be accomplished by even the smallest fraction of SME's, and by May of 2018, is simply foolish. However, many areas of GDPR can be addressed in a short timeframe and with the appropriate focus thereby reducing the risk to acceptable tolerance levels.

As a function of cyber underwriting in the EU, the following factors are greatly encouraged before a policy is bound.

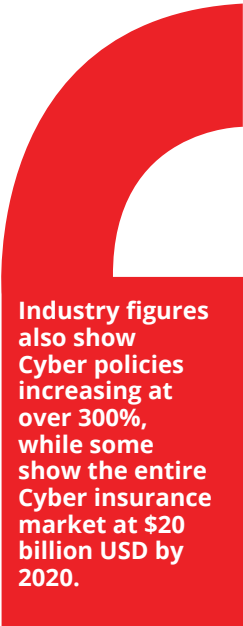
GDPR FOCUSED CONTROLS ASSESSMENT REVIEW

There are many industry assessments that are labeling themselves as GDPR

compliant, or GDPR driven, most of which focus solely on the technical safeguards rather than the actual organizational and system controls. The following questions should be included in any assessment that looks to provide a compliant score.

- ◇ If processing is based on implied consent, does affirmative consent get collected from data subjects and documented?
- ◇ What consent evidence does the processor have of personal data that is already processed?
- ◇ What systems does the entity have in place to erase the personal data of a data subject upon request?
- ◇ What system or mechanism does the entity have to provide the data subject's personal information on request in a commonly used, machine-readable format?
- ◇ Does the entity have a process or system to notify the relevant supervisory authority of a personal data breach without undue delay, and where possible within 72 hours?
- ◇ Does the entity have a process or system to notify data subjects about a data breach?

The assessment should follow on to ask the industry accepted controls review by the Center for Internet Security (CIS) v6.0 of the Security Controls. This assessment process covers (20) key security control areas that overlay perfectly on GDPR.



Industry figures also show Cyber policies increasing at over 300%, while some show the entire Cyber insurance market at \$20 billion USD by 2020.



DATA BREACH PREVENTION BASED CYBER SECURITY POSTURE

The second area of focus is on the existing security posture of the entity. In this area, the recommendation would be to ensure that the entity has taken steps towards **prevention** as opposed to remediation.

Several new technologies on the market offer a paradigm shift to cyber-attack prevention. Coupled with responsible service providers these “platform” based technologies can deliver a form of “GDPR in a Box”. These are discussed more fully in the Solution section. The key point is that any technology that does not form part of an overall multi-prevention approach is useless, and will not provide the insured with the levels of protection they require to remain secure and prevent breach.

Lastly, in addition to a multi-prevention platform, the system should have a robust machine learning detection and reporting platform.

RECOMMENDED TECHNICAL SOLUTIONS FOR GDPR COMPLIANCE



SOLUTION (GDPR IN A BOX)

The solution section of this whitepaper will focus on the solutions provided by Clarium Managed Services, utilizing enterprise grade products from Palo Alto Networks, and Splunk. Gartner Research leaders in their respective areas. Clarium has developed a rapid delivery system to bundle and make these technologies available to potential insureds in the EU for a cost effective monthly management fee.

There are (4) critical areas that Clarium, Palo Alto Networks, and Splunk can help with organizations' security and data protection efforts related to GDPR compliance by assisting in:

- **Assess+ GDPR.** Clarium is finalizing a new assessment platform this is built specifically for identifying GDPR compliance and providing a simple and easy to read score for the administrator. Besides the (6) GDPR areas specifically identified in the GDPR controls review, Assess+ will also include all (20) main areas of The Center for Internet Security (CIS) CRITICAL SECURITY CONTROLS, and lastly components from the ISO 27001. The most comprehensive scoring apparatus written for the GDPR utilizing international industry best practice's.
- **Securing personal data.** The GDPR requires security of data processing, accounting for the state of the art. Our Security as a Service Platform provides just that security at the application, network and endpoint level, as well as in the cloud.
- **Data breach prevention.** Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR. Proper cybersecurity is essential to ensure organization's personal and business-critical data and applications remain protected. Our Security as a Service Platform is built for prevention.
- **Data breach notification.** In the unfortunate instance of a data breach, it must be reported. Our Security as a Service Platform can help determine what personal data was compromised, and contribute key facts about measures taken to address the breach.

Proper cybersecurity is essential to ensure organization's personal and business-critical data and applications remain protected.

GDPR in a Box



1. ASSESS+GDPR

Assesses the (6) key areas of GDPR controls review plus the (20) main areas of the Center for Internet Security (CIS), Critical Security Controls. The most robust GDPR assessment on the market.



2. SECURING PERSONAL DATA

The GDPR requires security of data processing, accounting for the state of the art. Our Security as a Service Platform provides just that security at the application, network and endpoint level, as well as in the cloud.



3. DATA BREACH PREVENTION

Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR. Proper cybersecurity is essential to ensure organization's personal and business-critical data and applications remain protected. Our Security as a Service Platform is built for prevention.



4. DATA BREACH NOTIFICATION

In the unfortunate instance of a data breach, it must be reported. Our Security as a Service Platform can help determine what personal data was compromised, and contribute key facts about measures taken to address the breach.



www.clarium.tech

1 877 · THREAT · 0

SECURING PERSONAL DATA

The GDPR requires security of data processing, accounting for the State of the Art mandate. Palo Alto Networks platform secures data at the application, network and endpoint level, as well as in the cloud.

Truly reducing cyber risk and protecting data, including personal data, requires integrated, automated and effective controls in place to detect and prevent known and unknown threats at every stage of the attack lifecycle. Built from the ground up for prevention, the Clarium Security as a Service Platform allows organizations to confidently pursue a digital-first strategy as they implement key technology initiatives within the cloud and, increasingly, mobile networks to protect their most valued data assets from exfiltration by cybercriminals and accidental data leakage.

The Clarium Security as a Service Platform combines network and endpoint security with threat intelligence to provide automated protection and prevent cyberattacks – not just detect them. Our platform natively brings together all key security functions – including firewall, URL filtering, IDS/IPS, and advanced endpoint and threat protection. Because these functions are purposefully built into the platform with cyberthreat prevention in mind, and natively share essential information across the respective disciplines, our platform ensures better security than legacy firewalls and antivirus, UTMs, or point threat detection products. In short, better security supports better data protection.



**PREVENT
UNKNOWN
THREATS**

DATA BREACH PREVENTION

Prevention of data breaches, whether a result of hacking or accidental leakage, is crucial for compliance with the GDPR.

Proper cybersecurity is essential to ensure your organization's personal and business critical data and applications remain protected. Our platform enables four key prevention techniques relevant to data security, simultaneously contributing to GDPR compliance

- **Complete visibility.** Our platform offers visibility into all traffic – across the network, endpoint and the cloud – classified by application, user and content. You can't stop or protect against what you can't see. Complete visibility provides the context to enforce dynamic security policy. Coupled with event monitoring delivered by Splunk, Clarium Security as a Service delivers enterprise grade visibility to an organization at a reduced monthly subscription cost.
- **Reduce the attack surface.** The attack surface is expanding rapidly as companies' use of applications and devices (e.g., SaaS, cloud and IoT) proliferates. The more avenues available to infiltrate an organization, the more opportunities for a cyber adversary to exfiltrate personal data. Clarium can enforce a positive security model, reducing the attack surface by enabling only the allowed applications for the right users and denying everything else.
- **Prevent known threats.** Many data breaches result from known threats, such as commodity information-stealing Trojans, malware and application exploits. On the perimeter, our platform controls the threat vectors themselves through the granular management of all types of applications. This immediately reduces the attack surface of the network, after which all allowed traffic is analyzed for exploits, malware, malicious URLs, and dangerous or restricted files or content. On the endpoint, Clarium and Palo Alto Networks Traps™ combines threat intelligence from our global community of customers with our unique multi-

method prevention approach to block known malware and exploits before they can compromise endpoints.

- **Prevent unknown threats.** Our platform goes beyond stopping known threats to proactively identify and block unknown malware and exploits, which are often used in sophisticated and targeted attacks. When a novel malware or exploit is seen, the Palo Alto Networks Global WildFire™ cloud-based threat analysis service automatically creates and shares a new control to your prevention devices, like next-generation firewalls and Traps™ advanced endpoint protection, in as few as five minutes, without human intervention.

In addition, Traps deploys a unique, multi-method approach to block the core techniques used by zero-day exploits, identify, and block unknown malware from compromising endpoints.

These prevention techniques are powered by WildFire, the industry's most advanced analysis and prevention engine for highly evasive zero-day malware and exploits. The cloud-based service employs a multi-technique approach that combines dynamic and static analysis, innovative machine learning techniques and a groundbreaking bare metal analysis environment to detect and prevent even the most evasive threats. WildFire goes beyond legacy approaches used to detect unknown threats, bringing together the benefits of four independent techniques for high-fidelity and evasion-resistant discovery:

- **Dynamic analysis:** Observes files as they detonate in a custom-built, evasion-resistant virtual environment, enabling detection of zero-day malware and exploits using hundreds of behavioral characteristics.
- **Static analysis:** Effectively detects malware and exploits that attempt to evade dynamic analysis, as well as instantly identifying variants of existing malware.
- **Machine learning:** Extracts thousands of unique features from each file, training a predictive machine learning classifier to identify new malware and exploits in a way not possible with static or dynamic analysis alone.
- **Bare metal analysis:** Automatically sends evasive threats to a real hardware environment for detonation, entirely removing an adversary's ability to deploy anti-VM analysis techniques. Together, these techniques allow Clarium to discover and prevent unknown malware and exploits with high efficacy and near-zero false positives.

DATA BREACH NOTIFICATION (GDPR)

In the unfortunate event of a personal data breach, the GDPR requires notification to supervisory authorities, unless the event is unlikely to result in risk to individuals' rights or freedom. Notification must include a range of information, including what data was impacted and what measures were taken.

Our platform can help maintain compliance with this GDPR requirement in the event of a breach. For example, AutoFocus and Splunk provide the analytics details needed for remediation, helping to understand who the user was, what the threat was, the impact

and the level of risk. All of this can help with notification requirements.

In addition, the next-generation firewall can be used to educate users via custom notification pages. System administrators can add their desired education message to the notification pages so that whenever an accidental data leak is prevented, the end user is served that message. For example, the message can include a link to the corporate data policies and best practices. This helps with overall prevention, as well as education efforts that support notification.

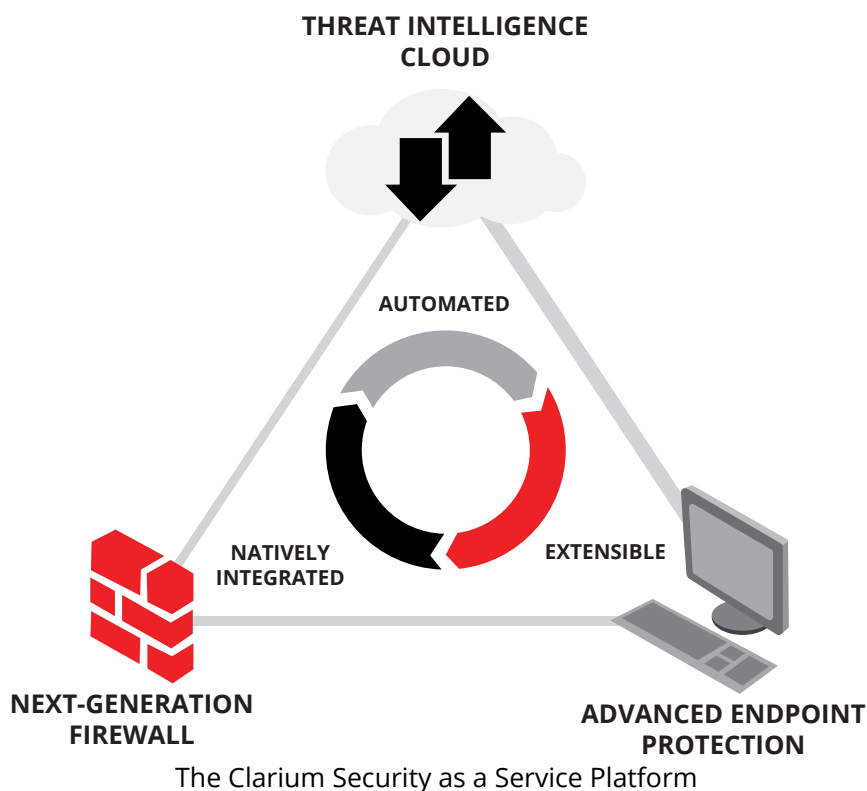
SUMMARY

Clarium has designed a breach prevention **platform** that provides all the key mandates required by the GDPR, and at a monthly subscription price point that provides underwriters with added confidence on new cyber policies. Particularly in the SME space.

Clarium's platform will allow insureds to enjoy award-winning products with 100% prevention rates, such as Traps, while significantly reducing the upfront cost of capital to deploy these products on premise. Notwithstanding the human capital cost and shortage, which must be factored in developing these mechanisms in house, Clarium's Security as a Service is clearly the appropriate solution to pursue.

Following the core mandates of GDPR should not be a process that disrupts a business operation, nor adds significant layers of information technology (IT). Unfortunately, many organizations are beginning to muddy the waters on the intent and solution to reach GDPR compliance. For example, many consultancies have recently suggested that encrypting data is in fact a requirement.

This process alone can place a significant burden on SME's when in fact the mandate is appropriate technical and organizational measures to ensure a level of security appropriate to the risk. This process can be achieved in a number of different "State of the Art" ways that removes the costly, cumbersome, and unnecessary method of encryption followed by decryption to an SME. Many of which are available as a service from providers like Clarium.





1 877 · THREAT · 0

www.clarium.tech