SECURING FINANCIAL DATA:

The Financial Sector and GDPR

logpoint

GDPR compliance and securing Financial Sector data

Since the turn of the millennium, the financial services industry has been no stranger to legislation, regulation and compliance. This has largely come about due to a series of catastrophic failures in business transparency, ultimately leading to the collapse of bankrupt giants such as ENRON and Lehman Brothers. Ever since, regulatory bodies and organisations have sought to work in greater partnership to help identify risk, exposures, fraud and illegal activity.

The industry has also witnessed the power of big data – with numerous financial institutions seeking to use these insights to better understand and serve worldwide markets. The sheer amount of data created globally in recent years is staggering, expected to rise from 4.4 zettabytes produced daily in 2013 to 44 zettabytes by 2020[1]. Beyond commercial insight, this information also provides organisations and regulators with the ability to detect potential danger and intervene in time to prevent a crisis. Wells Fargo, for example, utilises its big data lab[2] to both identify who is using their technologies and to better detect transaction fraud. The financial landscape is becoming increasingly complex, due not only to the amount of data to process but also the increasing requirements to keep it secure – a complexity exacerbated by the rise of cyber threats. In 2016 alone, 80 million cyber-attacks were detected against financial services – netting an estimated £8bn[3] through fraudulent transactions. Cyber-attacks therefore pose a direct threat not only to financial institutions, but also to the data they hold, which is frequently personally identifiable in nature. Despite holding a wealth of personal information, just one in five[4] financial service organisations are confident they could detect a data breach.

Finance: key challenges

When GDPR legislation comes into force in 2018, organisations will need to:

- **Know what data is held, its origin, and how it is utilised**
- **Understand how this data can be secured against potential breaches or accidental disclosures**
- **Identify how this regulation can be implemented whilst ensuring compliance with existing regulations**

Failure to do so could result in a fine of €20m, or 4% of annual turnover

GDPR – tougher new regulation on the horizon

The risks of unauthorised data disclosure range from damaging customers' financial situations to defamation of character and even revealing business trade secrets. To help businesses adapt to the new risks presented, new EU regulation is set to encourage greater transparency over the handling and storage of personally identifiable information (PII). The General Data Protection Regulation (GDPR), to be implemented on 25th May 2018, is set to standardise the way data is held and reported on across the EU. It will also introduce fines for non-compliance – €20m or 4 per cent of annual turnover – whichever is higher.

logpoint

This new regulation requires data breaches to be reported to relevant authorities within 72 hours; the employment of a Data Protection Officer; and policies to secure data portability. In short, this new regulation's primary objective is to strengthen and harmonise data protection for individuals as well as to simplify regulatory obligations, building upon existing regulations already in place.

The impact of GDPR implementation in finance

Prior to GDPR, financial institutions have an opportunity to implement processes, tools and technology – not only to ensure GDPR compliance, but to integrate best practice – directly translating to more effective operations. Beyond compliance, the benefits of the digital transformation encouraged by GDPR can deliver ROI from both a security and operational perspective. Key to implementation of the regulation in the financial services sector, however, is how GDPR will interact with existing financial regulations and best practices.

Compliance plus efficiency – using SIEM

SIEM highlights what is happening with an organisation's data. This helps to:

- Accurately report on transactions within finance, meeting compliance and increasing organisational efficiencies
- Normalise data streams, increasing efficiencies behind data analysis strategies

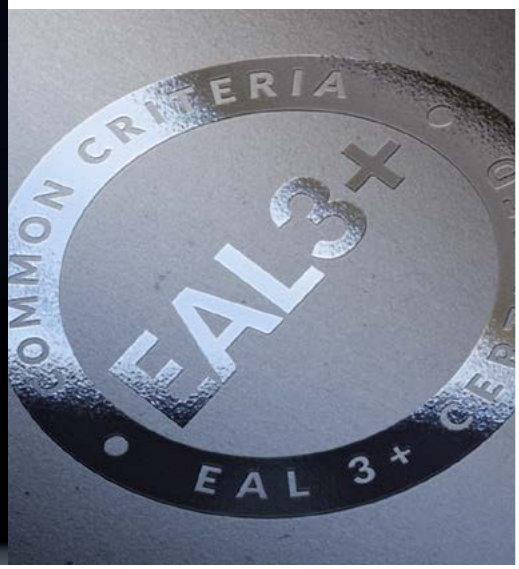
SIEM: the benefits

SIEM technology enables organisations to:

- Rapidly search, sort and analyse data – saving vast amounts of staff time
- Meet compliance around multiple complex requirements
- Proactively monitor networks, identifying and documenting security breaches early so they can be contained
- Utilise bespoke compliance reporting formats as standard

For example, under the Markets in Financial Instruments Directive (MiFID II), designed to remove barriers tot cross-border financial services through increased market transparency, financial organisations are required to record all conversations that have been made around a deal. Linking in to Bring Your Own Device (BYOD) policies, this regulation also incorporates all business calls made on personal devices. Notably, MiFID II specifies that any and all recordings must be stored for a minimum of five years, with requirements for regular Trades and Transaction reporting. GDPR and MiFID II combined will therefore result in a larger amount of PII stored, and greater financial repercussions should this data be stolen. The motivation behind ensuring accurate data reporting in finance are clear, with stringent fines for non-compliance. Barclays Bank, for example, was recently fined £2.45m[5] for failure to accurately report on 57.5 million transactions.

LogPoint enters global SIEM elite with top customer scores in Gartner Peer Insights



SIEM technology – normalising data; exceeding compliance

The sheer scale of data being utilised in the financial sector represents both significant risk and opportunity. The onus increasingly falls to finance professionals to ensure full awareness of exactly what data they are in possession of, where it came from, how it is stored, what the process for access is and what is being done with the data. By utilising an innovative SIEM solution, data from previously disparate systems can be normalised and collated in a single location, allowing information to be displayed, analysed and reported on with ease – far exceeding the requirements of compliance and integrating with existing analytic undertakings.

Where data loss may not have been identified due to alternative categorisations, the security intelligence SIEM provides can help identify data breaches, allowing a rapid response to minimise data-theft and fines from delayed, or inaccurate, reporting – key aspects to meeting compliance of both GDPR and MiFID II through secure storage. SIEM also possesses pre-emptive functionality, using data patterns from the collation of records to identify anomalies and help spot problems early on, before they have a significant impact.

With less than a year to go until implementation of GDPR, finance and IT professionals have an opportunity to review existing systems and ensure compliance is achieved ahead of schedule. This will help minimise exposure to risk, increase capacity for accurate, timely reporting, and normalise data streams for analytics purposes. LogPoint is a specialist in SIEM solutions, and prides itself in assisting organisations, including those in the finance sector, with their compliance and security requirements.

About LogPoint

Founded in Denmark in 2008, LogPoint is a SIEM specialist with over 300 clients across Europe. LogPoint's SIEM solution extracts value from data that companies already hold by collating millions of logs from disparate systems to extract meaningful information that businesses can act on.

Beautifully designed and intuitive to master, LogPoint prides itself in delivering the best SIEM solution on the market to make complex information easily accessible across all industries. Its SIEM software is NATO standard EAL3+ certified, one of only a small number of SIEM systems accredited to International Defence & Intelligence standards.

Headquartered in Copenhagen and deployed throughout Europe and Scandinavia, LogPoint has a dedicated UK team of technical experts on hand to help organisations get the best from SIEM technology.

VISIT: www.logpoint.com

EMAIL: uk@logpoint.com

PHONE: +44 (0) 203 893 3003

1) http://www.northeastern.edu/levelblog/2016/05/13/how-much-data-produced-every-day/
2) http://www.bizjournals.com/sanfrancisco/blog/2014/07/wells-fargo-bank-big-data-analysis-millennials-wfc.html
3) http://www.computerweekly.com/news/450413850/Cyber-criminals-net-8bn-from-financial-services-in-2016?utm_content=control&utm_medium=EM&asrc=EM_ERU_73429728&utm_campaign=20170301_ERU%20Transmission%20for%2003/01/2017%20(UserUniverse:%202313298)&utm_source=ERU&src=5614441
4) https://www.capgemini-consulting.com/resources/data-privacy-and-cybersecurity-in-banking-and-insurance
5) http://www.thetradenews.com/Regions/Europe/FSA-fines-Barclays-for-trade-reporting-failures/

logpoint