ELSEVIER

# computer FRAUD & SECURITY

ISSN 1361-3723 February 2015 www.computerfraudandsecurity.com

## Featured in this issue:

### Can the UK cyber-security industry lead the world?

**Due to costly and damaging hacking attacks, large companies, governments and individuals are increasingly concerned about cyber-security. This has led to the growth of a UK cyber-security sector estimated to be worth over £6bn.**

However, in order for the UK security industry to thrive, it needs continuous innovation and investment to keep pace. Andrew Tyrer of Innovate UK examines why the Government is interested in funding and supporting the growth of the cyber-security sector, the opportunities that exist for cyber-security companies, and the government support on offer.

*Full story on page 5…*

### A threat-based approach to security

**Traditionally, security practitioners are taught to evaluate security in terms of risk to their organisations, and security policies and practices are put in place purely to minimise these risks.**

The problem with this approach is that, by focusing on the 'worst case scenarios', we forget about the actual threats that exist. Security professionals and organisations need to change the focus from a risk- to a threat-based approach in order to stand the best chance against cyber-criminals, explains Will Semple of Alert Logic.

*Full story on page 7…*

### A proactive framework for automatic detection of zero-day HTTP attacks on educational institutions

**With the increased use of Information and Communication Technology (ICT) in educational institutes, security has become a big area of concern.**

Current signature-based intrusion detection provides only limited protection. Sanmeet Kaur and Maninder Singh of Thapar University, Patiala, India, propose a new hybrid automated signature generation system that is able to detect cross-site scripting, directory traversal, command injection and SQL injection attacks.

*Full story on page 10…*

### US health insurer Anthem hit by massive data breach

**Anthem, a major US healthcare insurer, has admitted to a data breach affecting 80 million customers and staff. That could make it one of the largest ever, and certainly the biggest in the healthcare sector.**

The story was still developing as this issue went to press, but the organisation has created a special website – www.anthemfacts.com – to post a message from president and CEO Joseph Swedish and a FAQ. At the time of writing, this offered no details about the nature of the attack other than characterising it as 'sophisticated', which is pretty much a standard response these days.

*Continued on page 3…*

## Contents

# Get ready for PCI DSS 3.0 with real-time monitoring

Joel John Fernandes

**Joel John Fernandes, ManageEngine**

**PCI DSS 3.0 compliance has gained worldwide acceptance by card service providers – card issuers, banks, and merchants – that plan to protect their customers' cardholder data from being misused. PCI DSS 3.0 has 12 security requirements concerning the protection of cardholder data. All businesses that accept, store, process or transmit customers card data either online or offline have to adhere to those requirements.**

## Most challenging

PCI DSS requirements 10 and 11.5 are considered to be the most challenging to fulfil for securing and protecting customers' payment card data from threats. Below are the descriptions for requirements 10 and 11.5 as found on the PCI Security Standards Council website.[1]

"Requirement 10: Track and monitor all access to network resources and cardholder data. Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimising the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult, if not impossible, without system activity logs.

"Requirement 11.5: Deploy a change-detection mechanism (for example, file-integrity monitoring tools) to alert personnel to unauthorised modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly."

PCI DSS requirement 10 pushes enterprises to gain security intelligence to know the 'who, what, where and when' of users accessing the network resources and cardholder data, whereas PCI DSS requirement 11.5 focuses on the protection of critical files from unauthorised access. In simple words, PCI DSS requirements 10 and 11.5 are put in place so that enterprises can easily analyse the complete user audit trail to identify:

- Who is logging into their systems.
- When they logged into the systems.
- What activities they carried out on the systems.
- Whether they accessed system files and other network resources.

To meet PCI DSS requirements 10 and 11.5, the log data generated by the network systems has to be collected at a central place and monitored in real time to track all anomalous activities happening on the network. IT environments consist of heterogeneous network devices, systems and applications that generate a huge amount of log entries every day. Manually monitoring log entries and critical files is impossible given the sheer volume of data that gets generated on a daily basis. Automation is the only solution to fulfil PCI DSS requirements 10 and 11.5.

## Automation framework

Let us now discuss the log data and file monitoring automation framework that businesses can implement to comply with PCI DSS requirements 10 and 11.5, thereby securing cardholder data and mitigating payment card fraud.

**Logging**: Identifying the network devices and systems that will be used to store, process, and transmit card data information is the first step to attaining PCI DSS compliance. Logging should be enabled for all network systems and devices that fall in the scope for PCI DSS, thereby allowing the IT security professionals to track and monitor all access to network resources and cardholder data. Relevant log information that is needed to comply with the PCI DSS requirements has to be enabled on all systems that fall in the scope for PCI DSS.

**Central log aggregation**: PCI DSS compliance requires enterprises to collect log data from network systems at a centralised place for effective reporting, security and analysis. IT security managers should have a universal log collection tool that can aggregate logs from heterogeneous sources – including Windows systems, Unix/Linux systems, applications, databases, routers and switches – at a central location.

**Continuous log reviewing**: Monitoring log data is not a one-time task that will keep you compliant with PCI DSS. IT security professionals should review their log data continuously to detect anomalous security events. Log analysis tools should be deployed so that the actionable security data is presented in graphs and charts on a dashboard. IT security managers should be able to quickly drill down into the data on the dashboard and perform a root cause analysis to identify why a security activity happened.

**Log retention**: Log data collected from all network systems must be stored for one year, per PCI DSS compliance requirements. Enterprises should archive, in a central repository, all log data

generated by network systems, devices and applications within their PCI DSS scope. Archived log data should be easily accessible for forensics investigation, thereby helping security professionals to drill down into the log data and perform root cause analysis to track down the event activity that caused the network problem.

**Log protection**: PCI DSS compliance mandates the protection of log data to avoid tampering and deletion. Enterprises should encrypt the log data files to ensure that the data is secured for future forensic analysis as well as compliance or internal audits. Hashing and time stamping can also be used to secure the log data and make it tamperproof. Log data can also be protected by using file integrity monitoring (FIM) solutions, as discussed in the next point.

**File integrity monitoring**: PCI DSS compliance dictates that enterprises use change-detection mechanisms such as file integrity monitoring tools to protect all sensitive data related to customers' payment cards. Security professionals need to centrally track all changes to their files and folders, such as when files and folders are created, accessed, viewed, deleted, modified, renamed and much more. File integrity monitoring tools allow IT security managers to make quick decisions when critical files are accessed and thereby mitigate the risk of payment card data breaches.

**Real-time alerting**: This is critical for enterprises. IT security professionals should receive alerts as and when network anomalies and suspicious activities occur on the network. Real-time security alerts help IT security professionals respond to critical incidents that can affect their network infrastructure. A delay in responding to such incidents can lead to a major security catastrophe. Deploying a real-time alerting solution that automatically monitors security events by mining the log data plays a vital role in PCI DSS compliance.

**User activity monitoring**: Customers' payment card data can be misused by employees who access the data using brute force attacks or by employees with privileged access. Monitoring user activities in real time across the IT infrastructure can be a painful task without proper user activity monitoring tools. PCI DSS compliance mandates enterprises to audit precise information in real time on critical user activity events such as user logons, user logoffs, failed logons, successful audit logs cleared, audit policy changes, objects accessed and user account changes.

## Automating to ensure compliance

Compliance with PCI DSS is a must for all businesses that accept card payments because keeping customer's payment card data secure is crucial for the progress of those businesses. PCI DSS compliance can bring enormous benefits to businesses such as a more secure network, higher brand value, improved reputation and lower risk of data breaches. Non-compliance, on the other hand, can have severe consequences.

Monitoring log data and critical files in real-time using the automation framework will help businesses to comply with the PCI DSS requirements 10 and 11.5 with ease.

### About the author

*Joel John Fernandes currently works as a senior product marketing analyst for ManageEngine. He has thorough knowledge in the log management and Security Information and Event Management (SIEM) domain and has consulted on nework security and log management for both large and small enterprises. He can be reached at joeljohn.f@manageengine.com.*

### Reference

1. PCI Security Standards Council, home page. Accessed Jan 2015. www.pcisecuritystandards.org.

# Coming full circle: are there benefits to BYOD?

**Sonia Blizzard, Beaming**

Sonia Blizzard

**Bring Your Own Device (BYOD) was kicked off by the smartphone and tablet revolution. As soon as everybody had their own powerful machine in their pocket workplaces deemed it useful to harness this power that we bring to work ourselves. In a stark contrast to 20 or even 10 years ago, when the only computer that we used was in the office, now we find ourselves carrying this equipment around with us and using the same technology at home as we do at work.**

## More flexibility

BYOD gives employees and employers more flexibility to complete their tasks at home, at work, during the commute or while waiting for a meeting. It also allows people to use mobile or cloud apps to share files and folders, as well as take advantage of the functionality offered by many smartphone and tablet apps on the market.

However, while the flexibility and functionality of BYOD is certainly enjoyed by many, and there are efficiencies for the employer, there are some serious risks that come along with bringing your own