PCI-DSS: A Million Dollar Risk for a 10-Cent Hacking Cost

COMPLIANCE, CALL RECORDING, AND NEXT-GEN HACKERS — A BUSINESS RATIONALE AND GUIDE TO PCI-DSS WITH ELEVĒO ACTIONS

Executive Summary — Million Dollar Risk for a 10-Cent Hacking Cost

There is a high probability that your company is out of compliance with the Payment Card Industry Data Security Standard (PCI DSS) because of stored cardholder data in contact center call recordings. The healthcare industry is particularly at risk with an estimated $6.2 billion cost of breaches.

So, what? The Real Costs and Risks

• Direct and indirect breach costs can be in the millions for smaller companies and over $100 million for large ones. Costs can include lawsuits, transaction processor fines, revenue drops, attrition, and remediation. The costs affect small, mid-sized, and big companies alike.

• Risk is greatly increasing because of the widespread availability of open source and "speech to text" cloud software, such as Amazon Transcribe or IBM Watson.i Using these tools, hackers can pull a credit card number out of a recorded audio file for as little as 10 cents.

Payment processors can fine acquiring banks $5000 to $100,000 per month for PCI DSS compliance violations, in addition to halting payment processing services.[ii] According to a 2018 report by Ponemon Institute, class action lawsuit settlements from companies of various sizes include:

DEFENDANT	SETTLEMENT*
Anthem	$115 million[iii]
Target	$39 million
Home Depot	$13 million
Advocate Medical[iv]	$5.5 million
Stanford Hospital	$4.1 million
St. Joseph Health System	$3 million
Emblem Health[v]	$575,000
Tampa General Hospital[vi]	$10,000

The Missing Key to PCI DSS Compliance:

Our view of the market is that too many companies overlook the most obvious and important way to protect cardholder data during calls which are recorded. The PCI DSS standard clearly states: do not store recorded credit card information. Simply put, solve the problem by not capturing cardholder data in the first place. Pause and resume functionality should be implemented within contact center applications to stop call recording when agents are required to collect cardholder information.

Who should read this Paper?

People whose job responsibilities put them in the PCI DSS scope, such as contact center managers, operations managers, compliance and IT professionals should read this paper. If your employees and agents collect credit card data or consumer information it is important for you to understand the options available to assist you in maintaining PCI DSS compliance. While there are a dozen high-level PCI DSS requirements[vii], this paper focuses on protecting data stored in voice and screen recordings.

WHITE PAPER OUTLINE

Chapter 1. The Apology No CEO Wants to Write

> Dear Customers,
>
> Your data was stolen. Sorry.
> By the way, it will cost us millions to fix this.
>
> Sincerely,
> The CEO.

Regardless of industry or company size, handling a breach of customer data is a painful, humbling and humiliating experience. In September 2017, Equifax CEO Richard Smith penned a heartfelt apology, published in USA Today, after a record-setting electronic breach of **143 million Equifax customers' data** at the hands of hackers:

> "Last Thursday evening we announced a cybersecurity breach potentially affecting 143 million U.S. consumers. It was a painful announcement because of the concern and frustration this incident has created for so many consumers. We apologize to everyone affected. This is the most humbling moment in our 118-year history."[viii]

The effects of the breach were a perfect storm for Equifax:

- Within six days, **15 million of the 143 million affected Equifax customers** visited the breach website[ix] and **11.5 million customers** enrolled in credit monitoring and identify protection.
- CEO Smith **testified in front of Congress four times** to reassure US citizens Equifax could protect customer data.
- The CEO **resigned** after 12 years with Equifax.[x]
- Equifax experienced a **25% drop in their share price** and an increase in **costs of up to $75 million** in the months following the breach. Wall Street predicts the cost to reach **$4+ billion**.[xii]

Again, It's NOT Just Large Companies at Risk

Customer data breaches aren't just a risk for large or well-known companies[xiii] like Target, whose CEO resigned after 35 years and whose profits dropped 46% amid the now famous breach[xiv]. Smaller companies like Elmcroft Senior Living are publishing press releases addressing breaches[xv]. Still other companies like the Cerebral Palsy Research Foundation of Kansas have received the type of coverage no company wants for breaches. Even small dental practices are not immune from delivering a "Notice of Data Breach" to the media and their patients.[xvii] CEO Michael Riggs of Jack Cooper Holdings Corp, states, "any CEO who's not putting this at the top of their priority list is crazy."[xviii]

$3.5 Million: The Average Cost of PCI DSS Class Action Lawsuits

On top of several record-breaking class action lawsuits in 2017—Target Corporation $18.5 million, Nationwide $5.5 million, Cottage Health Systems $2.2 million—a recent ALM cyberSecure conference panel predicts an increase in PCI DSS breach lawsuits "driven by two factors:

- Courts are making it easier for victims to sue companies that suffer a data breach.
- Regulators are probing firms more aggressively with the aim of levying large fines."[xix]

The IBM/Ponemon Institute 2017 Costs of Data Breach study estimates **an average breach cost of $3.5 million with a 27% probability that a U.S. company will experience a breach in the next 24 months.**[xx]

40 Lines of Code to Get Credit Card Data out of a Call Recording

"The rollout of EMV chip cards in recent years may have deterred criminals from making fraudulent in-store purchases" eMarketer Retail says, "but it hasn't stopped them dead in their tracks. They simply found a new target—call centers."[xxi] **It's only a matter of time before hackers marry a treasure trove of call recordings with a good transcription tool. At the push of a button hackers will have millions of names, birthdays, addresses, social security numbers, credit card numbers, PIN numbers and other verbally collected and verified data at their fingertips.**

The availability and pervasiveness of no-to-low cost applications and tools to software developers and hackers alike poses a real and imminent challenge to businesses. In fact, free, 40-line, open source software programs exist that work with Google's speech-to-text API to transcribe audio.[xxii] As an example, Nuance Communications was transcribing dictated audio about patients in a recent attack which cost them $92 million in lost revenue.[xxiii]

Chapter 2. The Five Major PCI DSS Financial Risks in the Contact Center

The five key financial risks in the contact center are 1) penalties for non-compliance, 2) legal and operational costs, 3) lost revenue from customer attrition, 4) loss of reputation and future revenue, and 5) costs of executive resignation and job replacement.

Again, these risks apply to all companies regardless of size. The average cost per breach for small businesses is now $20,752—up from $8600 in 2013.[xxiv]

1. Payment Processor Penalties for Non-Compliance

According to Verizon's 2017 PCI Compliance Report, 80% of qualifying organizations are not PCI DSS compliant. Moreover, of those that are, only 55% are compliant within a year after validation.[xxv] The risk of non-compliance doesn't end with satisfying the Security Standards Council requirements. Payment processors can fine acquiring banks $5000 to $100,000 per month for PCI DSS compliance violations, in addition to halting payment processing services.[xxvi]

2. The Legal and Operational Costs

Legal battles and insurance repercussions can be expensive. In cases like P.F. Chang Restaurants[xxvii], the insurer paid $1.7 million for cyber insurance. Costs mounted further when the insurer denied paying another $1.9 million to Bank of America Merchant Services, citing exceptions in the policy.

There are also direct and indirect Operational costs associated with breaches. Direct costs include: public relations, legal support, insurance premiums, financing costs, costs of disruption, mandatory customer credit monitoring, identity protection fees, and loss of intellectual property. Indirect costs include those associated with additional contact center staffing to handle anxious customer inquiries.

Many believe the recent, sweeping European legislation contained in the General Data Protection Regulation (GDPR) will also have a huge impact on the cost of breaches, "If data breaches remain at 2015 levels, the fines paid to the European regulator could see a near 90-fold increase, from £1.4bn in 2015 to £122bn."[xxviii] GDPR has global scope, impacting any business on the planet doing business with citizens of the European Union.

3. Lost Revenue from Customer, Partner, and Supplier Attrition

After a 2016 breach that exposed four million customer records, UK giant Talk Talk Group was fined £600,000, and revealed a loss of £60 million and 100,00 thousand customers.[xxix] Digicert cited an average loss of customers to increase 15% between 2013 and 2014 following a breach in personal data.[xxx] According to the Cisco 2017 Annual Cybersecurity Report:

- A loss of revenue was experienced by 29% of organizations.
- A loss of opportunities was experienced by 23%.
- A loss of customers was experienced by 22%.[xxxi]

4. Loss of Reputation and Future Revenue

After the organization moves past CEO apologies, lawsuits, and bad press, they face the fact that many customers are not coming back. Not only does the breach affect current revenue, but lifetime value. A 2016 survey of five countries (US, UK, Germany, Australia and Japan) by non-profit organization The Internet Society, found that 40% of customers would not do business with an organization that had exposed sensitive customer information."[xxxii]

5. Cost of Executive Resignation and Job Replacement

While CEOs at Yahoo! and Facebook kept their jobs, some say by a slim margin, senior executives in the legal and compliance departments at Yahoo! and Uber weren't so lucky.[xxxiiii] Compliance officers, IT directors and legal counsel are also likely to feel the consequences of a breach. According to CSO Magazine, a data breach that becomes public is a fire-able offense in 38% of companies, while 68% of organizations consider failing to meet regulatory compliance and associated fines and penalties as a reason for dismissal.[xxxiv] In addition to the individual risks and costs, companies must also bear considerable expense filling vacated positions.

Chapter 3. The Eye-Opener: It's Easier than Ever to Pull Data from Recorded Calls

Amazon Transcribe charges $0.0004 per second to convert audio to text, making it easy for hackers to transcribe a 4-minute audio recording for about ten cents ($0.10).[xxxv] Similar services are offered by Google Compute Engine, Microsoft Azure, and IBM Watson who compete with Amazon Transcribe. Vendors not only compete with their services, but strive to offer tools that make building transcription applications simpler. Software development kits are available in a variety of languages such as .NET, Javascript, Ruby, Go, PHP, Java, and Python. These tools empower hackers to build applications quickly and easily while abstracting the gory details and complexities of transcription applications.

For a hacker, all it takes is a simple search of a call transcription document to find the words "credit card" or look for numbers. In fact, there are several widely available tools, like the free, open source app PANhunt, which can search drives or files for credit card numbers.
One telemarketing firm recently exposed 400,000 call recordings to the public, and a 3rd party blew the whistle on them, reporting that there was both personal and credit card information in 17,000 of the calls.[xxxvi] This is an example of why the PCI Data Security Standard 2.0 supplement, Protecting Telephone Based Payment Card Data exists:

- It is a violation of PCI DSS Requirement 3.2 to store any sensitive authentication data, including card validation codes and values, after authorization even if encrypted.
- It is therefore prohibited to use any form of digital audio recording (using formats such as WAV, MP3, etc.) for storing CAV2, CVC2, CVV2 or CID codes after authorization if that data can be queried; recognizing that multiple tools exist that potentially could query a variety of digital recordings.
- Where technology exists to prevent recording of these data elements, such technology should be enabled.[xxxvii]

Chapter 4. The Most Overlooked Way to Protect Call and Screen Recordings

PCI DSS applies to any business, in any industry that processes credit card information over the phone. While there are a dozen high-level requirements, PCI DSS Requirement 3 mandates that users treat spoken PCI the same as written PCI and requires companies to dispose of the data or mask it in stored recordings. The best way to protect against capturing PCI DSS data is to PREVENT the call and screen recording[xxxviii] platform from recording it. If this information is not recorded in the system, then hackers cannot get to it.

There are three major avenues to prevention described below. In our view, number three is the most often overlooked while being the most cost-effective and risk-reducing option:

1. Ensure Agents don't Speak about or Show PCI Data

Contact centers can implement authentication, verification, and transaction processes that do not require agents to speak or display PCI data during calls. Sometimes this can be achieved through simple process reengineering. Companies simply can ask themselves, "Do we really need to ask for social security number AND birthday?". More often, it requires additional technology solutions such as IVR applications, 3rd party processing, and/or self-serve applications.

2. Manual Pause and Resume of Call Recordings

In this scenario, agents have access to buttons which control call recording status. Agents select the pause button to stop audio/video recording and press the button again to resume recording. While this doesn't typically create significant additional IT costs, the approach relies on the agent attentiveness. Agents have to pause and resume while simultaneously interacting with the customer and processing a transaction. Human errors here are common and put your PCI DSS compliance at risk.

3. Automatic Pause and Resume of Call Recordings

With automatic pause and resume, an agent's desktop application automatically triggers the call recording platform to pause and resume recording. For example, when an agent loads the billing transaction page in their application, the pause recording event is automatically triggered. Once the agent completes the billing transaction and moves to another area of the application, another trigger resumes the recording. The automatic triggers can be implemented in two ways:

- First, businesses can install an application that monitors activity on the agent desktop. These tools are programmed to learn where the cursor moves and lands for every possible set of pixels and applications on a screen. Upon recognizing pre-programmed scenarios, an API call is triggered to drive pause and resume functionality.

- Second, businesses can build tight integrations between recording platforms and billing applications. These integrations rely upon and developed using APIs published by both vendors. Pause and resume functionality is handled "behind the scenes" at the application layer and usually requires little or no additional installation of software on the agent desktop or back end.

The former of these two options is typically more expensive form both an implementation and support perspective. An engineer must train the "computer vision" to properly recognize the correct scenarios for pause and resume. Next, someone must install and test the functionality. Finally, any changes to the desktop environment, from software updates to new applications, require "re-training" and testing, making this a time consuming and labor-intensive option.

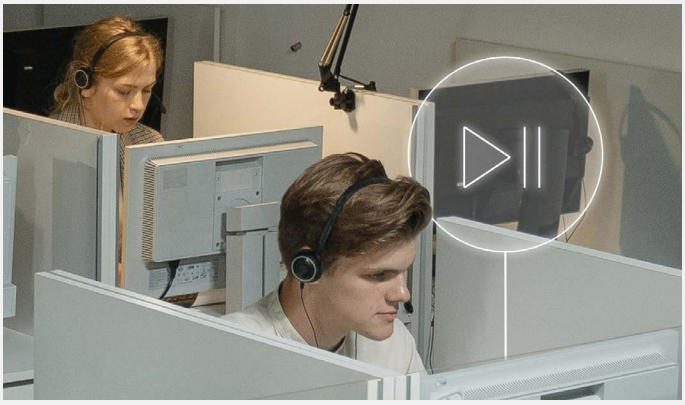
Elevēo highly recommends the latter option, as it is more simple and cost-effective to implement. If APIs exist, software developers build and test the integration once. Enabling the integration is as easy as configuration in admin interfaces. Changes to the agent desktop environment or other applications in the business ecosystem do not affect pause and resume functionality. Human, configuration, third party and back end errors are largely eliminated in the API integration approach.

Chapter 5. How Elevēo Supports PCI DSS with Pause and Resume

Elevēo is well known for its robust and flexible call and screen recording architecture. Customers describe Elevēo reliability as "Five nines of uptime" (i.e. 99.999% uptime) and "no server downtime for five years." Partners with leading contact center practices say, "unlike some competitors, Elevēo's software just works." While Elevēo provides complete support for all PCI DSS, HIPAA, GDPR, and MiFID II compliance initiatives, architectural capabilities, such as redundant recorders, will not be covered in this document.

Elevēo provides three key capabilities to support pause and resume functionality:

1. Open APIs for Pause and Resume
2. Connectors for Manual Pause and Resume
    a. Cisco Finesse
    b. Salesforce.com
3. Connectors for Automatic Pause and Resume
    a. Epic Systems Corporation (Healthcare)



Open APIs for Pause and Resume

Elevēo is a web-based platform with takes an API-first approach to building applications. What this means is that core functionality is built from the inside out in the form of open web services APIs. Simple SOAP or REST (XML) requests can be sent from ANY authenticated client application or service. Upon receiving API requests, Elevēo recorders can pause, resume, stop, start or retrieve recording status. In addition to the commands, the APIs will accept tagging of calls with ANY contact center meta-data, such as customer email, customer ID, case ID, or email address. Elevēo APIs are leveraged for all of the capabilities highlighted below. In addition, these APIs are extensible to integrate with the APIs of other vendors not specifically highlighted below.

Connectors for Manual Pause and Resume—Cisco Finesse and Salesforce.com

Manual pause and resume connectors expose recording control buttons to agents via their application user interfaces. These buttons are built with native Elevēo APIs described previously. Any application supporting Elevēo's web-based APIs can be customized with the manual pause and resume controls. Out of the box Elevēo has support for both Cisco Finesse gadgets and Salesforce.com widgets so that agents can control calls from those user interfaces.

Connectors built with Elevēo's APIs provide the following capabilities:

Recording Status: Displays the actual recording status of the agent's phone via visual cues directly in the agent's application.

Recording Control: Provides start, stop, pause and resume functions to enable the agent to control recording of a phone assigned to him.

Pre-Recording: Elevēo can be configured to cache all calls. When enabled. an agent on the phone with a customer can decide to keep a recording — even on already in-progress calls —and the platform will retain the entire call recording. If the agent decides not to record during the call, the cached recording is automatically deleted.

Tagging: Enables an agent to tag a call recording with meta-data, such as a pre-defined label in the Elevēo configuration or free form field. Tags can be wrap-up codes, notes, email addresses, customer IDs, case IDs, or anything of value to the business.

Transfer to Survey: Permits the manual transfer of an active call to an IVR voice survey with Elevēo Voice of the Customer.

Connectors for Automatic Pause and Resume—Epic

Automatic pause and resume integrations issue REST API requests programmatically to the Elevēo recording platform. Once built, these applications eliminate agent interactions with recording controls. Elevēo currently supports the innovative Elevēo Adapter for Epic Systems (healthcare industry application).

Elevēo has a very unique and innovative integration available to businesses in the healthcare industry. Customers who have already made an investment in Epic Systems can quickly and easily implement the Elevēo Automatic Pause and Resume for PCI app. The integration is built to work natively with Epic's billing system APIs. Once configured in the Elevēo and Epic application, any calls will pause and resume recording upon agent entry and exit from the Epic credit card billing interface. With this approach, there is no agent or application training required. More information on Elevēo Automatic Pause and Resume for PCI app is available in the Epic App Orchard marketplace. Long-term, the cost of developing a native integration, such as Epic, is well worth the time investment of valuable business resources.

Summary

From CEO-written apologies, class action fines, ruined reputations and careers — to the loss of customer and partner confidence, a breach of PCI DSS data should be at the top of every CEO and CIOs list of worst case scenarios. Emerging web-based technologies available to hackers make finding PCI DSS data in recorded calls easier, faster, and cheaper than ever. In order to mitigate this growing threat, the PCI DSS standards council has made it clear that where technology exists to eliminate PCI DSS data from call recordings, it should be used.

Elevēo continues to respond to the growing threats to customer data and the compliance initiatives that govern them, including PCI-DSS, HIPAA, GDPR, MiFID II and more. Elevēo is committed to developing innovations in functionality, architecture and technology through its API-first approach to application engineering. Our open APIs drive integrations with industry leading platforms such as Cisco, Epic and Salesforce.com. Automatic pause and resume is a critical strategy to create solutions that ensures air-tight compliance with PCI DSS requirements.

Elevēo is poised to help customers meet the many compliance challenges of today and well into the future. CEOs and CIOs can have complete confidence in the security of their contact center call recordings. Contact Elevēo today to discuss the options available to your business. Together we can build application ecosystems which help ensure that all call recordings are devoid of PCI data. The security of our customer data depends on it.

For more information, visit: www.eleveo.com

About Elevēo

Elevēo was formed to provide effective, simplified solutions for complex contact center problems.

Our products provide only features needed to elevate contact center operations & processes, are built using modern frameworks and cloud-native technologies that scale & move with your business.

Elevēo products are birthed from ZOOM International with its rich WFO history and award-winning products, services and reputation for service.

References

[i] Hacker Noon. (2017). Speech to text transcription in 40 lines of Bash – Hacker Noon. [online] Available at: https://hackernoon.com/speech-to-text-transcription-in-40-lines-of-bash-f466092d8feb [Accessed 4 Jul. 2018].

[ii] Merchant Link. (2014). How to Explain PCI Compliance Penalties to Beginners | Merchant Link. [online] Available at: http://www.merchantlink.com/how-explain-pci-compliance-penalties-beginners/ [Accessed 4 Jul. 2018].

[iii] NBC News. (2017). Anthem to pay record $115M to settle lawsuits over data breach. [online] Available at: https://www.nbcnews.com/news/us-news/anthem-pay-record-115m-settle-lawsuits-over-data-breach-n776246 [Accessed 22 May 2018].

[iv] Chicagotribune.com. (2018). Chicago Tribune - We are currently unavailable in your region. [online] Available at: http://www.chicagotribune.com/business/ct-advocate-settlement-privacy-0805-biz-20160804-story.html [Accessed 3 Jul. 2018].

[v] HealthITSecurity. (2018). EmblemHealth Data Breach Leads to $575K NY State Settlement. [online] Available at: https://healthitsecurity.com/news/emblemhealth-data-breach-leads-to-575k-ny-state-settlement [Accessed 3 Jul. 2018].

[vi] F5.com. (2018). Breach Costs Are Rising with the Prevalence of Lawsuits. [online] Available at: https://www.f5.com/labs/articles/cisotociso/breach-costs-are-rising-with-the-prevalence-of-lawsuits [Accessed 3 Jul. 2018].

[vii] Pcisecuritystandards.org. (2018). [online] Available at: https://www.pcisecuritystandards.org/pdfs/pci_ssc_quick_guide.pdf [Accessed 4 Jul. 2018].

[viii] Usatoday.com. (2018). [online] Available at: https://www.usatoday.com/story/opinion/2017/09/12/equifax-ceo-we-make-changes-editorials-debates/659738001/ [Accessed 4 Jul. 2018].

[ix] 2017 Cybersecurity Incident & Important Consumer Information. (2018). Cybersecurity Incident & Important Consumer Information | Equifax. [online] Available at: https://www.equifaxsecurity2017.com/ [Accessed 4 Jul. 2018].

[x] NBC News. (2017). The CEO of Equifax is stepping down in wake of epic breach. [online] Available at: https://www.nbcnews.com/business/consumer/equifax-ceo-richard-smith-retires-after-epic-breach-n804771 [Accessed 20 May 2018].

[xi] Fortune. (2018). Equifax Warns About Impact of Data Breach on its Business. [online] Available at: http://fortune.com/2017/11/10/equifax-warns-data-breach-business/ [Accessed 20 May 2018].

[xii] Money. (2018). Equifax's Massive Data Breach Has Cost the Company $4 Billion So Far. [online] Available at: http://time.com/money/4936732/equifaxs-massive-data-breach-has-cost-the-company-4-billion-so-far/ [Accessed 20 May 2018].

[xiii] Ocrportal.hhs.gov. (2018). U.S. Department of Health & Human Services - Office for Civil Rights. [online] Available at: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf [Accessed 4 Jul. 2018].

[xiv] Frizell, S. (2018). Data Breach Cuts Into Target Profits | TIME.com. [online] TIME.com. Available at: http://business.time.com/2014/02/26/target-credit-hacking-earnings-data/ [Accessed 22 May 2018].

[xv] Prnewswire.com. (2018). Elmcroft Senior Living Responds to Data Security Incident. [online] Available at: https://www.prnewswire.com/news-releases/elmcroft-senior-living-responds-to-data-security-incident-300662429.html [Accessed 4 Jul. 2018].

[xvi] Healthcare Analytic News. (2018). May: Another Banner Month for OCR-Reported Data Breaches (In a Bad Way). [online] Available at: https://www.hcanews.com/news/may-another-banner-month-for-ocrreported-data-breaches-in-a-bad-way [Accessed 4 Jul. 2018].

[xvii] Prnewswire.com. (2018). Michael Gruber DMD PA, Notice of Data Security Incident. [online] Available at: https://www.prnewswire.com/news-releases/michael-gruber-dmd-pa-notice-of-data-security-incident-300633368.html [Accessed 4 Jul. 2018].

[xviii] Fuhrmans, V. (2018). New Worry For CEOs: A Career-Ending Cyberattack. [online] WSJ. Available at: https://www.wsj.com/articles/cybersecurity-tops-priority-list-for-ceos-after-string-of-high-profile-hacks-1507821018 [Accessed 22 May 2018].

[xix] Janofsky, A. (2018). Why Companies Should Prepare for More Data Breach Lawsuits. [online] WSJ. Available at: https://www.wsj.com/articles/why-companies-should-prepare-for-more-data-breach-lawsuits-1512563334 [Accessed 21 May 2018].

[xx] Products, S., Accounts, M. and safe?, H. (2018). 2017 Payment Security Report | Verizon Enterprise Solutions. [online] Verizon Enterprise Solutions. Available at: http://www.verizonenterprise.com/verizon-insights-lab/payment-security/2017/ [Accessed 21 May 2018].

[xxi] eMarketer Retail. (2018). This Is the New 'Wild West' of Retail Fraud. [online] Available at: https://retail.emarketer.com/article/this-new-wild-west-of-retail-fraud/59010ebcebd4000a54864b37 [Accessed 21 May 2018].

[xxii] Hacker Noon. (2017). Speech to text transcription in 40 lines of Bash – Hacker Noon. [online] Available at: https://hackernoon.com/speech-to-text-transcription-in-40-lines-of-bash-f466092d8feb [Accessed 4 Jul. 2018].

[xxiii] Ragan, S. (2018). Nuance says NotPetya attack led to $92 million in lost revenue. [online] CSO Online. Available at: https://www.csoonline.com/article/3258768/security/nuance-says-notpetya-attack-led-to-92-million-in-lost-revenue.html [Accessed 4 Jul. 2018].

[xxiv] Pcisecuritystandards.org. (2018). [online] Available at: https://www.pcisecuritystandards.org/pdfs/PCI_SMTF_Infographic.pdf [Accessed 4 Jul. 2018].

[xxv] Products, S., Accounts, M. and safe?, H. (2018). 2017 Payment Security Report | Verizon Enterprise Solutions. [online] Verizon Enterprise Solutions. Available at: http://www.verizonenterprise.com/verizon-insights-lab/payment-security/2017/ [Accessed 21 May 2018].

[xxvi] Merchant Link. (2014). How to Explain PCI Compliance Penalties to Beginners | Merchant Link. [online] Available at: http://www.merchantlink.com/how-explain-pci-compliance-penalties-beginners/ [Accessed 4 Jul. 2018].

[xxvii] Policyholderinsurancelaw.com. (2018). Does Your Company Have Coverage for PCI Fines & Penalties in its Cyber Policy? | Neal Gerber Eisenberg's Insurance Policyholder Law Blog. [online] Available at: http://www.policyholderinsurancelaw.com/blog/does-your-company-have-coverage-pci-fines-penalties-its-cyber-policy [Accessed 4 Jul. 2018].

[xxviii] ComputerWeekly.com. (2018). UK firms could face £122bn in data breach fines in 2018. [online] Available at: https://www.computerweekly.com/news/450401190/UK-firms-could-face-122bn-in-data-breach-fines-in-2018 [Accessed 4 Jul. 2018].

[xxix] Theregister.co.uk. (2018). TalkTalk admits losing £60m and 101,000 customers after THAT hack. [online] Available at: https://www.theregister.co.uk/2016/02/02/talktalk_hack_cost_60m_lost_100k_customers/ [Accessed 22 May 2018].

[xxx] DigiCert. (2014). Customer Loss from Data Breach Is Rising | DigiCert Blog. [online] Available at: https://www.digicert.com/blog/cost-data-breaches-2014/ [Accessed 4 Jul. 2018].

[xxxi] Cisco.com. (2018). [online] Available at: https://www.cisco.com/c/dam/m/digital/en_us/Cisco_Annual_Cybersecurity_Report_2017.pdf [Accessed 4 Jul. 2018].

[xxxii] Internetsociety.org. (2018). [online] Available at: https://www.internetsociety.org/globalinternetreport/2016/wp-content/uploads/2016/11/ISOC_GIR_2016-v1.pdf [Accessed 21 May 2018].

[xxxiii] Fruhlinger, J. (2018). 8 security breaches that got someone fired. [online] CSO Online. Available at: https://www.csoonline.com/article/2859485/data-breach/the-buck-stops-here-8-security-breaches-that-got-someone-fired.html [Accessed 22 May 2018].

[xxxiv] Korolov, M. (2018). How to get fired in 2017: Have a security breach. [online] CSO Online. Available at: https://www.csoonline.com/article/3158825/it-jobs/how-to-get-fired-in-2017-have-a-security-breach.html [Accessed 22 May 2018].

[xxxv] Amazon Web Services, Inc. (2018). Amazon Transcribe Pricing – Amazon Web Services (AWS). [online] Available at: https://aws.amazon.com/transcribe/pricing/ [Accessed 4 Jul. 2018].

[xxxvi] Theregister.co.uk. (2018). Marketing company leaks 17,000 recorded phone calls, many with credit card numbers. [online] Available at: https://www.theregister.co.uk/2017/01/30/firm_that_leaked_13m_records_laughs_at_firm_that_leaked_400k_records/ [Accessed 22 May 2018].

[xxxvii] Pcisecuritystandards.org. (2018). [online] Available at: https://www.pcisecuritystandards.org/documents/protecting_telephone-based_payment_card_data.pdf [Accessed 4 Jul. 2018].

[xxxviii] Pcisecuritystandards.org. (2018). [online] Available at: https://www.pcisecuritystandards.org/pdfs/pci_fs_data_storage.pdf [Accessed 20 May 2018].