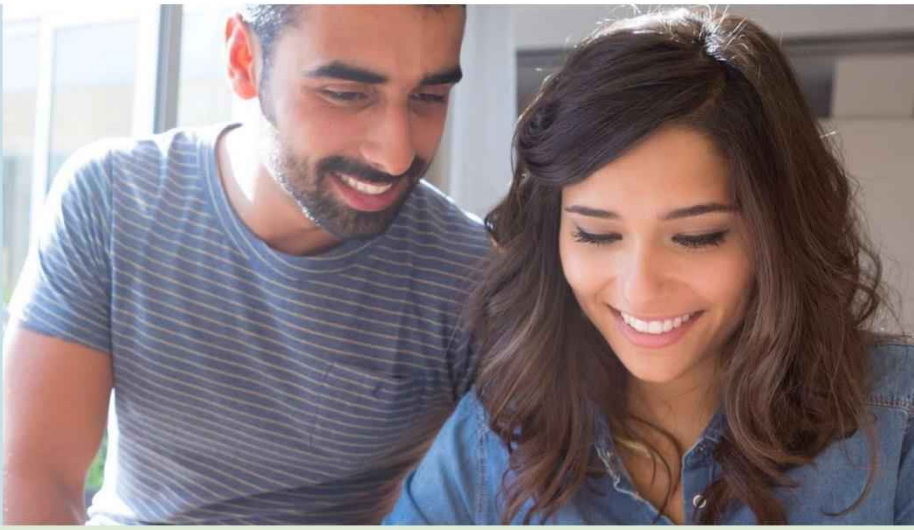
ASSOCIATION OF CARIBBEAN CORPORATE COUNSEL

Caribbean & Latin America Corporate Counsel Quarterly Newsletter

April 1, 2017



INTRODUCTORY LETTER FROM THE PRESIDENT OF THE ACCC

Welcome to the first issue of our quarterly e-newsletter. We will keep you informed of leading trends in the law regionally and internationally that affect in-house counsel in Latin America and the Caribbean (LAC) and of upcoming events and networking opportunities.

We look forward to seeing you at our upcoming 5th Annual Caribbean & Latin American Corporate Counsel Summit 2017 in Miami on November 16-17.

The LAC region is made up of diverse political and cultural environments. Given the growing number of in-house counsel supporting companies operating in both regions, this year we will be expanding to include coverage of the Latin American region. This will expose LAC in-house counsel to new networking opportunities and provide a greater understanding of the business and legal landscape of the LAC region.

The influence of in-house counsel on the legal landscape is constantly evolving and growing. Our role will be to continue to help you think ahead and plan for the future changes in the profession. If you not already a member, please email us today to sign up for membership.

Akerman

If you have suggestions for future topics or wish to write for our in-house counsel or regional section, we would love to hear from you. To unsubscribe from this newsletter, please reply to our email with **"UNSUBSCRIBE"** in the subject heading.

THE CYBERCRIME DILEMMA

Cyberspace represents the virtual world which brings people and places together creating a world without borders. These technological improvements have however created another avenue for criminal enterprise.

According to Interpol "cybercrime is a fast growing area of crime. Criminals are exploiting the speed, convenience and anonymity of the internet to commit a diverse range of criminal activities ... cause serious harm and pose very serious threats to victims worldwide". Put simply, any act in which the internet and information technology plays a substantial role for the commission of a criminal offence is known as a cybercrime.

Cybercrime is a growing concern in Jamaica. Prior to passing the Cybercrime Act 2010 there was no penalty for individuals who were participating or facilitating in harmful cyber activities. Based on a review and recommendations made, the 2010 Act was repealed and replaced by the Cybercrime Act 2015. The 2015 Act created new offences to keep pace with the evolution of cybercrimes. The 2015 Act sets out offences which may result in a person being liable on conviction. In addition to the prescribed penalties, the Court may order convicts to pay compensation to the victims.

Under the Act it is an offence to:

i. knowingly obtain unauthorized access to any program or data held in a computer (Section 3)

ii. access any program or data held in a computer with the intent to commit an offence or facilitate the commission of an offence punishable by imprisonment for a term exceeding one year. (Section 4)

iii. do any act which a person knows is likely to cause any unauthorized modification of the contents of any computer. (Section 5)

iiii. knowingly secure unauthorized access to any computer for the purpose of obtaining any computer service or without authorization intercepts or causes any function of a computer to be intercepted. – (Section 6)

v. without authorization or lawful justification or excuse, willfully cause a degradation, failure, interruption or obstruction of the operation of a computer or denial of access to or impairment of a program or data stored in any computer. (Section 7)

vi. fraudulently, with intent to procure an advantage for himself or another, to cause loss of property to another person by any input, alteration, deletion or suppression or data or any interference with any function of a computer. (Section 8a)

vii. fraudulently access any computer and input, alter, delete or suppress any data with the intention that the data be considered or acted upon as if that data were the original data. (Section 8b)

viii. use of a computer to send to another person any obscene data that constitutes a threat or is menacing in nature and is intended to cause or reckless as to whether the sending of the data, causes annoyance, inconvenience, distress or anxiety to that person or another person.

It is also an offence to facilitate the commission of the above offences by making computer devices or data available.

Under the Act a body corporate can be found liable for cybercrimes where it is found that a director, manager, secretary or similar officer of the company connives to commit the offence or failed to exercise due diligence to prevent its commission. The officer would also be liable on conviction in respect of that offence.

While the Act marks a step in the right direction, further improvement is needed to address issues such as cyberbullying, cybersecurity, electronic financial crimes and cyber extortion to name a few.

You Can Prevent a 'Panama Papers' Scandal at Your Law Firm

By Lou Shipley

Lou Shipley is Lecturer at the Martin Trust Center for MIT Entrepreneurship, MIT Sloan School of Management and CEO of Black Duck Software

The data breach at the law firm of Mossack Fonseca in Panama sent shock waves around the world in the spring with the prime minister of Iceland stepping aside, Swiss authorities raiding the headquarters of the Union of European Football Associations, and relatives of the president of China linked to offshore companies. The size of the breach was also shocking with 2.6 terabytes of data leaked. That's 30 times bigger than the WikiLeaks release or the Edward Snowden materials. However, the most shocking part of the "Panama Papers" story is that the breach and exploit of the popular open source project Drupal was totally preventable.

individual's estate plan, a startup's patent application, or a high-profile merger and acquisition, clients expect their information to be secure. Indeed, lawyers are required to keep this information both confidential and secure. Yet, despite the very high level of security owed this information, many firms lack an IT staff and outsource the creation and maintenance of their data management and security services. Once outsourced, there is an assumption that someone else will effectively manage the data and ensure its security.

This is many firms' first mistake. Even if they aren't managing their own IT, law firms still have an obligation to make sure that data is properly secured. This means asking frequent questions about security and ensuring that the vendor is implementing reasonable security measures.

This level of diligence is critical today, as law firms are increasingly under threat of attack. In March 2016 the international firms Weil Gotshal & Mangers and Cravath, Swaine & Moore reported data breaches, highlighting the risks for law firms and their clients. With the amount of confidential information retained by firms about business deals and strategies, there is an expectation of future attacks. Confirming this is a 2015 Citigroup Cyber Intelligence Center report cautioning big firms about the threat of attacks on their networks and websites.

This level of diligence is critical today, as law firms are increasingly under threat of attack. In March 2016 the international firms Weil Gotshal & Mangers and Cravath, Swaine & Moore reported data breaches, highlighting the risks for law firms and their clients. With the amount of confidential information retained by firms about business deals and strategies, there is an expectation of future attacks. Confirming this is a 2015 Citigroup Cyber Intelligence Center report cautioning big firms about the threat of attacks on their networks and websites.

Implementing reasonable security measures means continuously monitoring both proprietary and open source code for vulnerabilities. This is a notion that lawyers should be familiar with. In most M&A deals many lawyers advise clients to run security scans of the codebase to understand the code integrity and surface any vulnerabilities.
This is a particularly important M&A exercise for open source usage as much open source is not supported in same way proprietary software is — through automated updates and patches that are pushed out proactively. Still, open source code is the way software applications are built today and open source makes up 35 percent to 50 percent of the average code base so managing and securing it is vital. It is widely incorporated into programs used by law firms around the world. Open source tends to be high quality and offers powerful tools. However, you can't reap the benefits of open source programs without managing their risks.

This is a particularly important M&A exercise for open source usage as much open source is not supported in same way proprietary software is — through automated updates and patches that are pushed out proactively. Still, open source code is the way software applications are built today and open source makes up 35 percent to 50 percent of the average code base so managing and securing it is vital. It is widely incorporated into programs used by law firms around the world. Open source tends to be high quality and offers powerful tools. However, you can't reap the benefits of open source programs without managing their risks.

When a security vulnerability is identified in open source, it is publicly announced along with ways that the vulnerability can be exploited. Sometimes there is even a sample code or YouTube video giving cybercriminals a recipe for hacking. However, security updates and patches are usually made available too. Because the process is not automated, these announcements should be monitored and the patches installed promptly to ensure the security of data.

Sometimes this is easier said than done. Even when firms know open source software is used in their codebase, it can be difficult to know exactly where it exists. Without that visibility into what open source they're using and where, the patches aren't of much use. This is why it's critical for law firms to identify all open source code in use, inventory it, and map it to a known vulnerability database. When a vulnerability is announced, the firm can decide from a business standpoint if it's material and requires action. When it's deemed material, the stakes can be extremely high so scanning the code should be a regular compliance process.

Whether law firms have IT departments or outsource to a service provider, they should use products that automate the inventory process, monitor the software, and send automatic alerts when a security vulnerability is identified. It's not difficult to secure data when the right products are in place.

If Mossack Fonseca had such a procedure in place, the Panama Papers scandal never would have happened. The version of the open source project used, Drupal, had 25 or more known security vulnerabilities. They were publicly announced as far back as 2013. If anyone at the firm was paying attention, it could have implemented the security patches. When the patches weren't applied, it was open season for hackers.

The Panama Papers scandal illustrates the dangers of being lax about the security of client information. It also shows how law firms that take security seriously have a competitive advantage. As more data breaches are sure to come to light, law firms have an opportunity to differentiate themselves with a higher level of service. Those that don't could be the next hacking victim — or already are and just don't know it yet.

Common Reporting Standards

The Common Reporting Standard and Trusts

The Common Reporting Standard (CRS) is the standard for automatic exchange of financial account information (AEOI) developed by the Organisation for Economic Co-operation and Development (OECD). CRS draws extensively on the intergovernmental agreement (IGA) approach to implement the Foreign Account Tax Compliance Act (FATCA), and, similar to FATCA, requires financial institutions resident in participating jurisdictions to implement due-diligence procedures, to document and identify reportable accounts and establish a wide-ranging reporting process.

As of August 2016, over 100 jurisdictions have signed or were committed to sign the CRS. More than 50 jurisdictions are considered "early adopters," meaning that they will exchange information on financial accounts automatically starting in 2017. The remaining jurisdictions have committed to automatically exchange information starting in 2018.

Timing

Financial institutions that fall within the definition of a reporting financial institution in an early-adopter jurisdiction were required to implement CRS onboarding and due-diligence requirements starting January 1, 2016, to ensure that they captured the information needed to perform reporting in 2017. They also must complete a review of their high-value individual accounts by December 31, 2016 allowing them to report, at a minimum, new individual and entity financial accounts as well as high-value preexisting accounts in 2017. Remaining preexisting accounts must be reviewed by Dec. 31, 2017, and will be reported in 2018.

Differences between CRS and FATCA

Despite the fact that CRS draws extensively on the IGA approach of FATCA, there are key differences that require specific onboarding, remediation, and reporting enhancements. For example, the scope of CRS is broader than FATCA as it aims to identify tax residents in any of the 100+ jurisdictions participating in CRS and most thresholds applicable under FATCA do not apply for CRS. In addition, legal entity classifications can vary significantly from those under FATCA and the categories of entities that have to provide information on controlling persons is broader.

Finally, unlike FATCA, CRS does not impose a withholding requirement. Instead, CRS enforcement will be handled by each of the jurisdictions adopting CRS that will be required to establish an audit and penalty regime to encourage compliance with the rules.

Another important challenge associated with CRS is that even though the standard intends to impose uniform requirements across the jurisdictions adopting this new global information reporting regime, the reality is that each jurisdiction is entitled to exercise different options and expand the minimum requirements in the standard. Also, residency definitions and data privacy and protection rules can vary from country to country.

Treatment of Trusts

Most trusts will be considered Investment Entities (and therefore, Financial Institutions) under CRS if their gross income is primarily attributable to investing, reinvesting, or trading in financial assets provided they are managed by another Financial Institution. Being managed by another Financial Institution is defined very broadly and includes having a professional trustee or a trustee that hires any other entity as service provider such as a custodian, investment advisor, portfolio manager or any type of person involved in the investment, administration or management of financial assets. Generally, the only trusts that would not fall within the financial institution category are those which do not hold financial assets or whose trustee is an individual that does not hire any entity as service provider to perform any of the activities described above. Trusts that are Financial Institutions will need to identify their reportable accountholders (all classes of beneficiaries) and provided the required information to the participating jurisdiction.

Common Reporting Standards

In the event that the trust is not a financial institution, it will be considered a Passive NFE and will need to provide self-certifications for the trust with this CRS classification as well as for each Controlling Person. Controlling Person in the case of a trust will be each settlor, trustee, protector, beneficiaries or classes of beneficiaries, or any other natural person exercising ultimate effective control over the trust. Each Controlling Person will need to sign its own CRS self-certification.

CRS Look through Rule

The CRS look through rule requires reporting financial institutions to treat an account holder that is an investment entity managed by another financial institution (including a Trust Company) that is not a participating jurisdiction financial institution as a passive nonfinancial entity (NFE) and to document and report the controlling persons of the entity that are reportable persons. It should also be noted that according to the CRS Commentaries, each of these controlling persons needs to sign (or positively affirm) its own information.

The United States has neither signed nor committed to sign CRS instead indicating that it will achieve equivalent levels of reciprocal exchange through FATCA. CRS requires competent authorities of the participating jurisdictions to publish a list that identifies participating jurisdictions for the purposes of CRS look through provisions with respect to controlling persons of investment entities that are nonparticipating jurisdiction financial institutions. None of the lists released at this point recognize the United States as a participating jurisdiction. This means that the United States is likely to be a nonparticipating jurisdiction for most countries and therefore subject to the look through provision. Trusts in the United States, generally will be treated as investment entities managed by another financial institution. Therefore, U.S. Trusts may fall within the scope of the passive NFE definition and may need to identify their controlling persons and will likely need to provide self-certifications from each of them.

Thus, when U.S. trusts have financial accounts in a participating jurisdiction, they will need to provide self-certifications for both the entity and the controlling persons to the counterparty where they maintain the accounts.

CRS also seeks to attract investment entities incorporated in nonparticipating jurisdictions into participating jurisdictions, by requiring that a nonparticipating entity that is a trust and has a trustee in a participating jurisdiction will be treated as a participating entity. In other words, a trust established in the United States will be considered a reporting financial institution in a participating jurisdiction if any of its trustees are tax resident in a participating jurisdiction, regardless of the court and control test that applies in the United States to establish the tax residency of the trust. This would mean that the trust would need to comply with the due diligence and reporting requirements in the participating jurisdiction.

Implications

Due to the complexity of the rules, trusts established inside and outside the United States should undertake an assessment of the CRS rules and determine how they are affected. Knowledge of how other countries have adopted the standard may allow financial professionals to provide beneficial guidance to their clients on how to follow reporting and compliance rules in participating jurisdictions.

Cyber Security (In House Counsel Section)

Why is Cybersecurity Essential?

Authors: Kevin Haywood Crouch & Jacqui Sanaghan

In this growing technological era, more and more electronic data is being stored, with individuals and businesses making use of new technological advances on a daily basis. However, it is predicted that there are approximately 1 million victims of cybercrime per day and whilst the impact on individuals may be damaging, the impact on businesses can be staggering. This makes it imperative that businesses assess the safety of their data (client and proprietary) and understand their data protection responsibilities and those of their employees. For example, if you are holding your client's sensitive details and your systems are successfully breached, by external or internal attack, who bears the responsibility?

With data leaks, such as the 'Panama Papers' and the number of huge corporations falling victim to 'hacking' recently, it proves that even the large corporations aren't safe from data breaches and cyber-attacks. This issue doesn't just affect these corporations, however, smaller local businesses are at risk and have fallen victim to cybercrime in recent years too.

Cybercrime and data breaches can have a long-term impact on businesses. Aside from the obvious business disruption and reputational damage, companies can face having to respond to data protection or confidentiality breaches, intellectual property and other losses and often subsequent legal proceedings – all of which can pose huge financial implications for a business.

Some of the most common outsider attacks are hacking (unauthorised remote access); malware (the use of software designed to carry the hidden function to steal and send data); phishing (the use of fake, but legitimate seeming branded emails, websites and telephone calls, in order to request/gain personal and confidential information); denial of service attacks, including the use of ransomware (designed specifically to interrupt services, such as websites and email services – allowing time for an attacker to enter the system, or hold system access to ransom).

From a preventative perspective, IT related cyber security measures can be implemented to reduce the probability, and most importantly the impact, of a cyber-attack or breach. Measures, such as independent data vulnerability and information security reviews, which are now being requested by insurers as payouts in relation to data loss/theft increase, are recommended. Such impartial security reviews allow gaps or inadequacies to be identified and remedied. Other active measures such as 'Intrusion detection and prevention systems' and firewalls that detect and prevent attacks, are also recommended.

Such preventative measures can ensure a quick response to an incident, preserving data and systems, identifying the source of the attack and reducing its impact. Thereafter remediation and disaster recovery planning will further reduce the impact in the event of a cyber-attack or data leak incident.

INTERNATIONAL LEGAL UPDATES

Cyber Security (In House Counsel Section)

Just as important however, are employee and board level awareness and understanding of the risks. This understanding is just as key to protecting your business and clients. The highest risk often comes from those within the business, whether intentionally or unintentionally, employees can often leak information or destroy data or systems, as well as enable outsider attacks. Some of the most vital, but also most cost effective, cybersecurity measures relate to the implementation of tailored cyber-threat policies and procedures, including user awareness training that ensures that employees throughout the business have an awareness of all the main cyber risks and their individual responsibilities for them.

Whilst an organisation is always responsible for understanding the ethical and legal requirements in relation to their data, and for implementing adequate preventative and recovery measures and policies, it's always the individual employee's responsibility to ensure that they adhere to these policies and stay vigilant. Enforcing good habits, such as locking PCs, ensuring passwords and data are not left lying around and are disposed of properly, showing caution when clicking on links and reporting any incidents can make a huge difference. Therefore it is always a combination of prevention, detection, adequate recovery planning and organisation-wide education that proves the best defence against the threat and impact of cybercrime.

Kevin Haywood Crouch is the Global Head of Forensics and Consulting, and Jacqui Sanaghan a Forensic Technology manager for KRyS Global, an international fraud investigation, dispute resolution and regulatory compliance firm with 50 professionals working from eight offices worldwide, predominantly situated in offshore financial centers.

For more information contact :

kevin.haywoodcrouch@krys-global.com P: +1 345 947 4700
jacqui.sanaghan@krys-global.com P: +1 345 947 4700

Events:

- **May 19** | ***Trinidad***
  BANKRUPTCY & INSOLVENCY SEMINAR 2017
- **May 26** | ***Trinidad***
  FACTA/CRS
- **September 22** | ***TBA***
  1ST ANNUAL LEGAL OFFSHORE SUMMIT 2017
- **November 16-17** | ***Miami***
  5TH ANNUAL CARIBBEAN & LATIN AMERICAN CORPORATE COUNSEL SUMMIT 2017