CorporateLiveWire

FRAUD & WHITE COLLAR CRIME 2018

VIRTUAL ROUND TABLE

www.corporatelivewire.com

Introduction & Contents

The Fraud & White Collar Crime Roundtable 2018 addresses the latest trends and interesting developments in several key jurisdictions. We discover why compliance may be a "daunting" but "necessary" task in 2018. Understand the implications of noteworthy case studies, including the anti-corruption case against Rolls-Royce and a record-breaking settlement following the prosecution of a former British Formula 1 race official. Other highlighted topics include: Deferred Prosecution Agreements, cross-border fraud, cybersecurity, and recent regulatory developments and criminal trends. Featured countries are: Australia, Germany, Romania, and United States.

James Drakeford
Editor In Chief

8 1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

11 2. What international conventions apply in your jurisdiction?

12 3. Have there been any recent regulatory changes or interesting developments?

14 4. Can you outline the key fraud and white collar crime trends?

18 5. Have there been any other noteworthy case studies or examples of new case law precedent?

19 6. What complications or difficulties arise from cross-border fraud & white collar crime?

22 7. What are the main benefits and drawbacks of a DPA [Deferred Prosecution Agreement] scheme?

24 8. To what extent has a changing technological landscape and professionalisation of cyber criminals altered the way in which information security is delivered?

27 9. What measures can be implemented to help minimise risk following a security breach?

29 10. How can companies ensure they get the balance right between implementing risk management and risk prevention?

31 11. In an ideal world what would you like to see implemented or changed?

USCOV Attorneys at law

SIEMENS Ingenuity for life

stetter maximum protection

NAVIGANT

NYMAN GIBSON MIRALIS Criminal Defence Lawyers and Advisors est. 1966

AlixPartners when it really matters

KRyS Global Complex Issues. Resolved.

MEET THE EXPERTS

Susan Markel - Alix Partners
T: +1 (202) 756-9016
E: smarkel@alixpartners.com
W: www.alixpartners.com

Susan oversees matters involving corporate financial reporting, regulatory investigations, whistle-blower actions, Foreign Corrupt Practices Act (FCPA) enforcement, and internal controls. Formerly at the US Securities and Exchange Commission (SEC), she served as chief accountant of the enforcement division. She has a Bachelor of Science in accounting from the University of Akron, is a CPA and certified in financial forensics. Susan has received several awards including the SEC's Distinguished Service Award in 2006 and The National Law Journal's 2014 "Governance, Risk and Compliance Trailblazer and Pioneer". She is a speaker nationally and internationally on public reporting and accounting related to financial fraud investigations and other enforcement actions involving the SEC and other government entities.

Kenneth M. Krys - KRyS Global
T: +1 284 494 1768
E: Kenneth.Krys@KRyS-Global.com
W: www.KRyS-Global.com

Kenneth Krys is a qualified and licensed insolvency practitioner in the Cayman Islands, the British Virgin Islands and Bermuda with 25 years experience in a range of corporate recovery, forensic accounting and regulatory compliance assignments. He has overseen the liquidation of a number of high profile and complex cross-border engagements in the Caribbean, including BCCI, SPhinX and Fairfield Sentry. He was Head of Compliance (Enforcement) of the Cayman Islands Monetary Authority from 2002 - 2004 and was part of the Deloitte team that assisted the Thailand Government with their financial services viability review in 1997 and 1998.

Ken is a Chartered Accountant, Chartered Financial Analyst, Certified Fraud Examiner, Certified Anti-Money Laundering Specialist, Certified Specialist in Asset Recovery and Chartered Business Valuator.

He is Vice-President of the Cayman Islands Compliance Association (CICA) and is acting President of local chapter #123 of the Association of Certified Fraud Examiners (ACFE). He was a former council member of the Cayman Islands Society of Professional Accountants (CISPA) serving on the Investigation and Compliance Sub-Committees, and currently sits on the CISPA Insolvency Practitioners Sub-Committee.

Further, he is a member of INSOL International, American Bankruptcy Institute (ABI) - serving on its Caribbean Insolvency Symposium Board of Advisors, The International Association for Asset Recovery and the Restructuring and Insolvency Specialist Association (BVI) Limited. Ken has provided expert evidence in a number of litigation matters, has written various articles and speaks frequently at conferences and symposiums.

Alma Angotti - Navigant
T: +1 202 481 8398
E: alma.angotti@navigant.com
W: www.navigant.com

Alma Angotti is a Managing Director in the Global Investigations & Compliance practice. A widely recognized anti-money laundering ("AML") expert, she has trained and advised the financial services industry as well as other regulators and government officials worldwide on AML and combating the financing of terrorism ("CFT") compliance. Ms. Angotti has an extensive background as an enforcement attorney conducting investigations and litigating a variety of enforcement actions.

Dennis Miralis - Nyman Gibson Miralis
T: +61 2 9264 8884
E: dm@notguilty.com.au
w: www.notguilty.com.au

Dennis Miralis is a leading Australian defence lawyer who acts and advises in complex domestic and international criminal law matters including:

- white collar and corporate crime
- money laundering
- serious fraud

Dennis Miralis specialises in representing clients in transnational /international criminal law matters such as assets forfeiture proceedings involving multiple jurisdictions (including China, Hong Kong, Singapore, South Korea, Russia, the UK, Canada, Europe, the USA and Mexico) as well as the following areas of transnational / international criminal law:

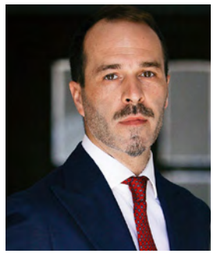
- International money laundering law
- International Proceeds of Crime law
- Bribery and corruption law
- Transnational crime law
- Cybercrime law
- Extradition law
- Mutual Assistance in Criminal matters law

He appears in all courts throughout Australia and regularly travels outside of Australia for complex international / transnational criminal law matters.

MEET THE EXPERTS

Sabine Stetter - Stetter Rechtsanwalte
T: +49 89 13 92 791-0
E: s.stetter@stetterlegal.com
W: www.stetterlegal.com

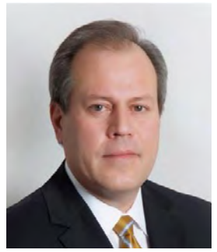
Dr. Sabine Stetter, Managing Partner at Stetter Rechtsanwälte, studied law at Ludwig-Maximilians-University in Munich and at the London School of Economics. From 2000 to 2003 she worked in criminal appeal proceedings before the Federal Supreme Court in Karlsruhe. For more than 15 years she has devoted herself exclusively to criminal business and tax law and founded Stetter Rechtsanwälte in 2010. Dr. Stetter's doctorate in criminal tax law concerns an evaluation between German and American law systems in this respect. Furthermore, Dr. Stetter is one of the co-authors of the "Münchener Anwaltshandbuch Strafverteidigung" (a standard reference work for German defence counsels). She is a member and speaker of the International Bar Association, the American Bar Association and the American Chamber of Commerce in Germany.



Adrian Uscov - USCOV | Attorneys at Law
T: +40 728 305 561
E: adrian.uscov@uscov.eu
W: www.uscov.eu

Adrian Uscov is Founding Partner of USCOV | Attorneys at Law and specializes in business crime and white collar defence, particularly in cases instrumented by specialised criminal investigation units such as National Anticorruption Directorate (DNA) and the Directorate for Investigating Organized Crime and Terrorism (DIICOT). Throughout his career he consolidated his knowledge and practice in both business and criminal law in what would gradually become the pillars of his expertise in business crime.

USCOV | Attorneys at law offers legal advice of the highest quality in a broad range of practices, looking at matters from multiple angles and routinely collaborating across practices, enabling them to efficiently and creatively solve complex client problems.



Robert N. Sikellis - Siemens AG
E: robert.sikellis@siemens.com
W: www.siemens.com

Robert N. Sikellis assumed his current position as Chief Counsel Compliance for Siemens AG on October 1, 2014, based in Munich, Germany. In this capacity, Mr. Sikellis leads the Compliance Governance Organization for the legal Compliance management, Compliance policies, internal investigations, disciplinary sanctions and remediation and Compliance in Mergers and Acquisitions.

Prior to assuming his current position, Mr. Sikellis held a number of other leadership roles within Siemens, including most recently Senior Vice President & General Counsel of Siemens North East Asia and Siemens Ltd., China. In this function, he was responsible for all legal and compliance in the region and was a member of the Leadership Team in the region. Before China, Mr. Sikellis was General Counsel, Regional Compliance Officer and Member of the Board of Directors for Siemens AE (Greece), based in Athens, Greece, as well as at Siemens AG Headquarters in Munich, Germany, where he was assigned to the Legal & Compliance organization.

Prior to joining Siemens in 2008, Mr. Sikellis was Associate General Counsel and Managing Director for a large U.S.-based consulting firm. He remained in this position for over 10 years, handling the full range of commercial and corporate issues facing a large consulting corporation.

Previously, Mr. Sikellis was the Chief of the Attorney General's Special Criminal Investigations Division based in Massachusetts (USA). As Chief Director of the Special Criminal Investigations Division, he oversaw and supervised all investigations and prosecutions for the Division, including the High Technology Crime, Narcotics, Organized Crime, Arson and Asset Forfeiture Units. Prior to being appointed Chief Director, Mr. Sikellis was an Assistant Attorney General assigned to the Attorney General's Special Criminal Investigations Division, where he prosecuted hundreds of criminal cases, ranging from complex white collar to organized crime to money laundering offenses.

Until 2002, Mr. Sikellis was also an Adjunct Professor at Boston University School of Law, where he taught advanced trial advocacy. Mr. Sikellis, an American citizen, is a cum laud graduate of Boston University and Boston University School of Law and is admitted to practice law in the United States of America.

1. In your jurisdiction, what are the main regulatory provisions and legislation relevant to (i) corporate or business fraud, (ii) bribery and corruption, and (iii) insider trading?

Uscov: In Romania the main regulatory provisions related to the subject are contained in the following normative acts:

- Criminal Code (Law no. 286/2009)
- Law no. 78/2000 on the prevention, detection and sanctioning of corruption acts
- Law no. 297/2004 on the capital market
- Law no. 656/2002 on the prevention and sanctioning of money laundering
- Law no. 241/2005 for the prevention and combating of tax evasion
- Company Law No. 31/1990
- Law no. 11/1991 regarding unfair competition

The Romanian Criminal Code and other special laws on different matters criminalise active and passive bribery, including bribery of foreign officials, and sanctions corruption. Special provisions are dedicated to offences against the financial interests of the European Union in Law no. 78/2000 on the prevention, detection and sanctioning of corruption acts.

Other examples of corporate or business fraud are provided in: Article 241 of the Criminal Code regarding bankruptcy fraud, Article 242 of the Criminal Code regarding fraudulent management, Article 245 of the Criminal Code regarding insurance fraud and even in the Chapter IV of Criminal Code regarding fraud committed using computer systems and electronic payment methods.

Also the acceptance, use or traffic of money, valuables or any other assets managed or administrated by a person, on their or on another person's behalf is punishable according to Articles 295 and 308 Criminal Code (embezzlement). Law no. 241/2005 against tax evasion has special provisions in this matter, with a particularity: all tax crimes have the requisite mental state direct intention (in order to avoid the fulfilment of tax obligations).

Article 5 Law no. 11/1991 regarding unfair competition established that the disclosure, acquisition or use of commercial secrets by third parties as a result of a commercial or industrial espionage action if the interests or activity of a legal person is affected is punishable.

A company can be held criminally liable for these offences committed by individuals acting on its behalf.

Stetter: Fraud is regulated by law in Germany in Section 266 StGB (German Criminal Code). The provision does not differentiate between corporate or business fraud and other cases of fraud. Under German Law three different forms of bribery and corruption can be found in the German Criminal Code:

- Sections 299 to 302 – addressing bribery in business dealings and the health sector;
- Sections 331 to 337 – covering bribery of public officials; and
- Sections 108b to 108e – concerning bribery in connection with elections.

Within the scope of these provisions the law distinguishes between active and passive bribery.
Section 38 WpHG sanctions violations of the prohibition on insider trading and the prohibition of market manipulation.

Sikellis: In Germany, we have recently seen laws passed prohibiting corruption in the healthcare arena and, more broadly in the European Union, amendments designed to better fight international corruption. The impact of these changes remains to be seen.

In June 2017, the German legislature amended its antitrust laws to include, in alignment with European Union legislation, additional sanctions against companies. The new laws also make it more difficult for companies to escape administrative fines by simply changing their company structure. Additionally, these changes make it easier for both companies and individual customers to pursue antitrust-based damage claims.

More generally, last summer Germany introduced a new law to assist in securing assets obtained from illegal acts, even well after they were committed, in order to return those assets to victims.

Miralis: The main legislation relevant to corporate and business fraud in Australia is the Commonwealth Criminal Code 1995 (Cth) (the Criminal Code) which broadly criminalises a range of dishonest conduct such as medicare fraud, tax fraud, and financial transactions fraud.

One of the more frequently used offence is s.134.2(1) of the Criminal Code – the offence of obtaining a financial advantage by deception which carries a maximum term of imprisonment of 10 years. The bribery offence provisions are also found under the Criminal Code and carry terms of imprisonment up to 10 years. Both domestic and foreign bribery of public officials is criminalised. The Code applies to corporations and individuals alike.

Generally breaches of the Code are investigated by the Australian Federal Police (the AFP) and prosecuted by the Commonwealth Director of Public Prosecutions

(CDPP) Criminal offence provisions relating to fraud are also contained in the Corporations Act 2001 (Cth) with a focus on fraud by Directors of Corporations, falsification of books, dishonest use of position and carrying on a financial service without a licence.

The main corporate regulator is the Australian Securities Investments Commission (ASIC) which regulates Australia's corporate environment and administers the Corporations Act including prosecutions for insider trading. The penalties for insider trading include large financial penalties and a maximum term of imprisonment of 10 years.

Additionally, there is Australia's financial intelligence unit, the Australian Transactions Reports and Analysis Centre (AUSTRAC) which appears to be playing an increasing role in regulatory prosecutions, initiating high profile investigations and court proceedings against a number of large Australian financial institutions in 2017 for breaches of Australia's AML laws.

Markel: In the United States, the Foreign Corrupt Practices Act is the primary law relevant to bribery and corruption. It was enacted in 1977 and has both anti-bribery provisions (Section 30A of the Securities Exchange Act) and books and records provisions (Section 13(b) of the Securities Exchange Act).

While there was a lull in activity for many years, since the mid-2000s, there has been a steady rise in enforcement cases related to bribery and corruption as well as new laws covering these areas in many other countries including the United Kingdom and Brazil. For public companies, the Securities Exchange Act of 1934, and specifically, Rule 10b-5, and the Securities Act of 1933, specifically section 17(a)(1), addresses fraud whether it be related to financial reporting, market manipulation, improper investment sales practices or insider trading.

> *"As a member of the Group of States against Corruption that was set up by the Council of Europe in 1999, Germany is part of the international community that monitors states' compliance with anti-corruption standards."*
>
> *- Sabine Stetter*

2. What international conventions apply in your jurisdiction?

Uscov: The most important and relevant international conventions applicable in Romania are:

- The Criminal Law Convention on Corruption, adopted in Strasbourg on 27 January 1999, ratified by Romania through Law no.27 / 2002
- The Civil Convention on Corruption, adopted in Strasbourg on 4 November 1999, ratified by Romania through Law no.147 / 2002
- The United Nations Convention Against Corruption, adopted in New York on 31 October 2003, ratified by Romania through Law no. 365/2004
- European Convention on Laundering, Detection, Seizure and Confiscation of the Proceeds from Crime, Strasbourg, 8 November 1990, ratified by Law no. 263/2002
- Council of Europe Convention on Cybercrime, Budapest, 21 November 2001, ratified by Law no. 64/2004
- European Convention on the Protection of the European Communities' Financial Interests EU
- Convention Against Corruption Involving Officials, adopted 1997, Romania acceded to convention in 2008.

Stetter: As a member of the Group of States against Corruption that was set up by the Council of Europe in 1999, Germany is part of the international community that monitors states' compliance with anti-corruption standards. Furthermore, Germany is a signatory to the following international treaties on anti-corruption:

- the OECD Anti-Bribery Convention;
- the United Nations Convention against Corruption;
- the Convention on the protection of the European Communities' financial interests
- the Council of Europe's Civil Law Convention on Corruption (awaiting ratification); and
- the Council of Europe's Criminal Law Convention on Corruption (since 1 September 2017)

3. Have there been any recent regulatory changes or interesting developments?

Uscov: Romania currently has some draft normative acts, which are currently being discussed in the Parliament, regarding the introduction of thresholds from which certain deeds are to be considered crimes, facts that are currently qualified as crimes, but for which, if the projects will be adopted, sanctions will be of a different nature than criminal.

The internal development is in accordance to EU's legislative development, as it has been recently adopted the Directive (EU) 2017/1371 of the European Parliament and of The Council of 5 July 2017 on the fight against fraud to the Union's financial interests by means of criminal law, which establishes in Article 7 the following: "where a criminal offence referred to in point (a), (b) or (c) of Article 3(2) or in Article 4 involves damage of less than €10,000 or an advantage of less than €10,000, Member States may provide for sanctions other than criminal sanctions".

Stetter: The new Sections 299a and 299b of the StGB have been in force since June 2016, governing bribery and corruption in the healthcare sector. Numerous cooperative practices – as used in the past by pharmaceutical companies and medical professionals, for example – became illegal with this change in the law. As a consequence, the courts will have to determine where the exact borderline between legal and illegal cooperation can be drawn over the coming years.

Furthermore, for a number of years it has been observed throughout Germany that prosecution authorities have tended to pursue transgressions more frequently and have adopted a tougher stance. A noticeable development is the gradual shift towards a privatisation of anti-corruption measures. Measures taken by private companies – e.g., compliance management, internal investigations and self-disclosure – are becoming increasingly important. About half of all investigations in this field are initiated based on company-provided evidence. Therefore, self-regulation in the economic sector is becoming an extremely important pillar when it comes to triggering the prosecution of white collar crimes.

Sikellis: There has been a potentially significant regulatory development in the U.S. During a speech on 29 November 2017, Deputy Attorney General Rod Rosenstein announced a new policy with respect to FCPA cooperation. Mr. Rosenstein said that when a company sufficiently self-discloses misconduct, cooperates fully, and timely and appropriately remediates the conduct, there will be a presumption that the Department will decline to prosecute the company. According to Mr. Rosenstein, this presumption could only be overcome if certain aggravating circumstances were present. This is a significant change in FCPA enforcement and a strong inducement to self-report corruption. It will be very interesting to see whether this policy extends to other areas.

Miralis: Australia is experiencing an active period of legislative reform covering white collar crime which is likely to continue into the next 12-18 months as a number of important pieces of proposed legislation are debated and introduced by the Federal Government.

Broadly speaking, the changes are in the areas of white collar crime and include changes to foreign bribery laws; the introduction of deferred prosecution agreements; whistleblower protection in the private sector; increased powers of the corporate regulator ASIC to investigate and prosecute breaches of the corporations law; an increase in the available penalties applicable to white collar/corporate crime and changes to the anti money laundering laws to regulate bitcoin exchanges.

Many of these reforms have been on the horizon for some time. The focus of the regulatory and legal changes is to address some of the perceived challenges involved in the detection and prosecution of white collar crimes.

Additionally, in late 2017, the Federal Government announced a Royal Commission into Banks which will be given significant powers to examine alleged bank misconduct in the banking, superannuation and financial services industry. These changes will better align Australia's domestic laws with international developments that have already taken place across the Europe and in the United States in recent years.

Krys: International organisations like the FATF, OECD and EU Council continue to exert pressure to address their concerns about fraud and taxation. As a result, there has been no shortage of regulatory changes in the offshore world. In many of the jurisdictions where we operate, we have recently seen regulatory revisions or new regulations in the following areas:

- Data privacy
- Beneficial share ownership
- Tax information sharing
- Anti-money laundering and terrorist financing
- Anti-corruption
- Freedom of information access
- Criminal Facilitation of Tax Evasion

Regulators in some jurisdictions have also started to take a different approach to enforcement by publically naming licencees in breach of regulations and publishing fines. In civil litigation, we have seen helpful guidance from the courts on such matters as the powers and authority of liquidators to pursue matters outside the jurisdiction, costs that may be taxed against a non-party of litigation, the duties and obligations of service providers to funds and the recognition of foreign receivers.

Markel: Over the last few years, we have seen the SEC emphasize in speeches and enforcement actions the need for a strong internal control environment – in some cases, the message being delivered is that they will not shy away from pursuing situations of "an accident waiting to happen" instead of waiting for the collision to occur.

Furthermore, we have seen an increased focus by the SEC on ensuring that the environment that gave rise to violations is appropriately remediated. Recently, the SEC has required companies in settled actions and as part of Deferred Prosecution Agreements to engage independent consultants and/or installed monitors if they are not convinced that issues have been sufficiently addressed by the company.

In the FCPA space, breakdowns in internal controls are often the crime that is being charged, particularly in instances where the final recipient of alleged improper payments cannot be proven. Going forward we can also expect to see an intense focus on cybersecurity and cryptocurrency – from both the regulatory and enforcement perspective.

4. Can you outline the key fraud and white collar crime trends?

Uscov: Romania is under supervision of the European Commission which annually issues the Cooperation and Verification Mechanism Report ("Report"). The Commission's 2014, 2015 and 2016 Reports have highlighted a positive trend and a track record pointing to strong progress and growing irreversibility of reform and this trend is confirmed in the 2017 Report, with a continued track record for the judicial institutions and a strong impetus by successive governments to strengthen corruption prevention.

Romania has allocated a lot of resources to discovering and sanctioning corruption acts under investigation by the National Anticorruption Directorate (DNA), such as (i) corruption offences (taking and giving bribe, traffic of influence, receiving of undue advantages), (ii) offences assimilated to those of corruption: establishing a diminished value for the goods belonging to the economic agents in which the state or an authority of the local public administration is a shareholder, committed during forced execution, judiciary reorganisation or liquidation; granting credits or subsidies by infringing the law or the crediting regulations; using the credits or subsidies for other purposes than those for which they had been granted; using a leadership position in a party or in a political formation, in a trade union or in employer's organisation or within a legal person without patrimonial purpose, with a view to obtaining money, goods or other undue advantages, and (iii) offences in direct connection with those of corruption: the concealment of goods originating in the perpetration of a corruption offence or of an offence assimilated to corruption; money laundering; abuse of office; fraudulent bankruptcy; tax evasion; traffic of drugs; traffic of people and so on.

Stetter: Regarding white collar crime the theme of corruption has been and will remain in sharp focus in Germany and new red lines have been drawn in what were formerly legal grey areas. However, the fight against corruption cannot be won at the legislative level; the crucial point is law enforcement. Companies and law enforcement authorities have to ask themselves how, for example, the Dieselgate scandal could remain undetected for such a long time despite existing compliance systems, ombudspersons and whistle-blowers.

Huge potential for damage also exists beneath the threshold of corruption, for instance through lobbying. One example is the so-called 'Cum-Ex' scandal, which over a decade led to significant financial damage (estimates go up to €32 billion). It can, at least in part, be attributed to the intensive lobbying of the finance industries' associations that the case did not come to light earlier. The trend towards privatisation of criminal prosecution makes law enforcement authorities increasingly dependent on company informants, suspect notifications concerning money laundering or internal investigations, which implies obvious risks. Overall, the fight against corruption can be expected to remain a significant challenge in the foreseeable future for legislators, law enforcement authorities and companies. There is hope, however, that the increasing digitalisation and automation of transactions, making them more traceable, could result in greater transparency in future.

Miralis: The key white collar crime and fraud trend appears to be a shift towards an increase in criminal penalties and providing the regulators and law enforcement with more powers to investigate and prosecute white collar crime. This has been accompanied by the recognition of the harm that such offences create to Australia's economy and a recognition that the penalties for white collar crime have to date not adequately reflected the objective seriousness of such offending. We are also likely to continue to see heightened activity by ASIC against banks who may have had failed to properly comply with their obligations to regarding issuing credit and for breaches of Australia's AML regime along with increased powers in the areas of exchange of information and the ability to freeze assets.

Additionally, the Australian Federal Police are being provided with more resources and training to investigate international fraud matters. The new proposed bribery laws have been drafted to broaden the offence of bribery of a foreign public official by creating a new strict liability offence for failing to prevent foreign bribery. The amendments to Australia's AML laws will ensure that "bitcoin exchanges" will be regulated and will impose reporting and record-keeping obligations on digital currency exchange providers, and require them to enrol and register on the Digital Currency Exchange Register maintained by Australian Transaction Reports and Analysis Centre (AUSTRAC) and to comply with protocols to identify and mitigate the risks of money laundering and terrorism financing. A Bill to establish an Australian Home Affairs portfolio was introduced into the Australian Parliament on 7 December 2017 which is likely to lead to centralisation of federal agencies working more collaboratively to investigate sophisticated white collar crimes including those with an international dimension. As Australia's key intelligence agencies and law enforcement agencies will now come under this new portfolio there will be a significant increase in the investigative capacities to detect serious financial crime.

> *"The tips received from whistleblowers following the enactment of rules pursuant to the Dodd-Frank Act has significantly increased since the SEC's rules provide for whistleblower protection"*
>
> *- Susan Markel*

Markel: There is always a sufficient number of potential financial fraud cases for the government to pursue. Historically, revenue recognition has been the largest area where this occurs as company's seek to hit topline growth and also EPS targets. These schemes include improper timing of revenue recognition, hidden side agreements that would preclude sale treatment and simply fictitious revenue. Other areas where fraud can occur relates to improper capitalisation of expenses, delayed recording of asset impairments, inadequate or misleading disclosure and earnings management. Identification of these cases can occur through a company's own due diligence and self-reporting or through the reports of a whistleblower to the SEC. The tips received from whistleblowers following the enactment of rules pursuant to the Dodd-Frank Act has significantly increased since the SEC's rules provide for whistleblower protection and the payment of a bounty for tips that lead to a successful SEC enforcement action where the money the SEC can recover through fines and disgorgement exceeds $1 million (for example, in FY 2017 alone the SEC received approximately 4,400 whistleblower tips).

Angotti: Key fraud and white-collar crime trends include:

(i) U.S. Economic Sanctions Violations

The use of economic sanctions will continue to be the "tip of the spear" of U.S. foreign policy. To that end, we believe that vigorous enforcement of sanctions laws and regulations will continue. For instance, the DOJ and OFAC's settlements with the Chinese telecommunications firm ZTE required joint efforts of the Department of Justice ("DOJ"), Department of Commerce ("DOC"), and Department of Homeland Security ("DHS").[1]

(ii) Money Laundering/Countering Financing of Terrorism

Anti-money laundering ("AML") actions will likely continue following 2017 criminal resolutions and regulatory actions against large global banks.[2] Given the national security implications, authorities would have a difficult time justifying lax enforcement of AML and sanctions violations.

As is typical after a natural disaster, federal and state prosecutors and regulators will be concerned about potential fraudulent activity related to disaster relief efforts in the wake of recent hurricanes and wildfires. Schemes can involve benefits fraud, fraudulent charities and cyber fraud.[3]

(iii) Corruption/Asset Recovery

Anti-corruption/anti-bribery enforcement and asset recovery of corruption proceeds will likely continue. This past year, 19 individuals pled guilty or were convicted in Foreign Corrupt Practices Act ("FCPA") related investigations. On 29 November 2017, the DOJ Deputy Attorney General announced the FCPA Pilot Program would be incorporated into the US Attorney's Manual.[4] Similarly, the government appears committed to finding and recovering the proceeds of corruption. For example, the U.S. DOJ filed a lawsuit to recover around $540 million in assets allegedly stolen from Malaysia Wealth Fund 1MDB, established by Prime Minister Najib Razak.[5]

(iv) Cybercrime

Information security is a top priority for companies and criminals. Information security breaches can occur through spearphishing,[6] business email compromise,[7] malware[8] and can originate from an insider as well. Private reports peg the average cost of a data breach at over $3.6 million. One large retailer reported spending $291 million in breach-related expenses. Breaches sometimes drive smaller businesses into bankruptcy.[9]

(v) Intellectual Property

Trademark counterfeiting, copyright piracy and other forms of intellectual property rights infringements are found in virtually every industry sector, and often result in significant risks to consumers worldwide as well as causing harm to the global economy,[10] and helping to fund organised crime, terrorism, and the trafficking of drugs, people, sex and wildlife.[11]

1. Treasury Department Reaches $100 Million Settlement with Zhongxing Telecommunications Equipment Corporation, March 7, 2017 - https://www.treasury.gov/press-center/press-releases/Pages/sm0023.aspx

2. Deutsche Bank, Agricultural Bank of China and Commerzbank AG; Federal Reserve Board Announces $41 Million Penalty and Consent Cease and Desist Order Against Deutsche Bank AG, May 30, 2017 - https://www.federalreserve.gov/newsevents/pressreleases/enforcement20170530a.htm
DFS Fines Agricultural Bank of China $215 Million for Violating AML Laws and Masking Potentially Suspicious Financial Transactions, November 4, 2016 - http://www.dfs.ny.gov/about/press/pr1611041.htm
Commerzbank AG Admits to Sanctions and Bank Secrecy Violations, Agrees to Forfeit $563 Million and Pay $79 Million fine, Thursday, March 12, 2015 - https://www.justice.gov/opa/pr/commerzbank-ag-admits-sanctions-and-bank-secrecy-violations

3. FinCEN Advisory FIN-2017-A007. October 31,2017 - https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2017

4. Deputy Attorney General Rosenstein Delivers Remarks at the 34th International Conference on the Foreign Corrupt Practices Act, November 29, 2017 - https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-34th

5. U.S. Seeks to Recover Approximately $540 Million Obtained from Corruption Involving Malaysian Sovereign Wealth Fund, June 15, 2017 - https://www.justice.gov/opa/pr/us-seeks-recover-approximately-540-million-obtained-corruption-involving-malaysian

6. An electronic communication scam targeting an individual, organization or business intending to steal data or install malware on the targeted user's computer.

7. Scammers target and trick employees with access to company finances to make wire transfers to partner held bank accounts, but the bank accounts are owned by the criminal.

8. Refers to various software with malicious intent including ransomware, viruses, worms and trojan horses.

9. Deputy Attorney General Rod J. Rosenstein Delivers Remarks at the Global Cyber Security Summit, London, United Kingdom, October 13, 2017 - https://www.justice.gov/opa/speech/deputy-attorney-general-rod-j-rosenstein-delivers-remarks-global-cyber

10. Department of Justice and Department of State Launch Intellectual Property Law Enforcement Coordinators Network, December 15, 2017 | Press Release Number: 17-1423 - https://www.justice.gov/opa/pr/department-justice-and-department

11. Fake fashion fuels vast illegal profits, funding terrorism and trafficking, thestar.com, February 28, 2017 - https://www.thestar.com/business/2017/02/28/fake-fashion-fuels-vast-illegal-profits-funding-terrorism-and-trafficking.html

5. Have there been any other noteworthy case studies or examples of new case law precedent?

Stetter: One of the most sensational and still most talked about cases is the prosecution of a former British Formula 1 racing official. Before an indictment, his case got laid off by the payment of a record-breaking sum of about €85 million which created a great stir. It is not only the scale of the payment that has provoked a discussion on the limits of terminating proceedings but also the anomalies in justice that the procedure might create. A bank official who accepted a payment made by the accused was punished with a lengthy prison sentence. Even though the case was concluded more than three years ago it is still omnipresent and, in current discussions, serves as a prime example for concerns about the status quo.

Sikellis: Over the last year, multijurisdictional anti-corruption actions by regulators have certainly been common. The settlement announced between the DOJ / SEC and Swedish company Telia relating to FCPA violations in Uzbekistan is particularly noteworthy because it constitutes the biggest settlement and disgorgement ever in an FCPA case. Another case is the $800 million fine for Rolls-Royce to settle with UK, US, and Brazilian anti-corruption authorities for bribe payments made throughout Africa, Asia, the Middle East, and Brazil. Notably, the Rolls-Royce fine and settlement stemmed from multijurisdictional collaboration of various regional anti-corruption authorities. I would expect to continue to see enforcement actions against international conglomerates as regulators expand their global policing of FCPA offenses.

These resolutions also reflect what appears to be a trend in how the DOJ and SEC are reaching global settlements with companies accused of FCPA offenses. Regulators are now willing to impose a total penalty on a named FCPA defendant, but then allow that total to be offset by amounts paid to enforcement authorities in other countries. In the Telia case, for example, the deferred prosecution agreement specifically permitted the total penalty to be reduced by the amounts paid to Dutch and Swedish authorities.

Krys: We have been involved in three matters recently that are noteworthy. One involved the sale of an asset in the United States and obtaining court's direction to disapprove the sale pursuant to section 363 of the U.S. Bankruptcy Code. The second was an Eastern Caribbean Court of Appeal decision on the ability of defendants to litigate in the U.S. to seek the BVI court's intervention to either stop or injunct proceedings commenced by a liquidator in the U.S. The last is the recognition of a Receiver of a segregated account appointed in one offshore jurisdiction in another jurisdiction.

These are all important as one of the most helpful remedies for gaining access to information and assets is via the insolvency rules. Accordingly we see the developments of insolvency case law precedent as helpful in progressing the ability of professionals like ourselves to investigate frauds, collect evidence and recover assets for victims.

6. What complications or difficulties arise from cross-border fraud & white collar crime?

Stetter: In parallel or consecutive procedures covering different jurisdictions, the course and the result of the proceedings in one country may have decisive influence on the respective proceedings in another country. Depending on the circumstances, the effects need to be considered in prior or parallel proceedings. This is even more important in light of an ever closer international cooperation between authorities. In these cases it is indispensable to create an overall strategy that combines as many relevant aspects from as many relevant jurisdictions as possible.

Miralis: From a defence perspective one of the main complications in the investigation of cross border fraud and white collar crime is the need to acquire a detailed understanding of the laws governing fraud offences, data exchange, extradition, mutual assistance and the right to silence, across multiple jurisdictions, which often can have very different laws covering these areas and sometimes different legal system altogether. The above areas of law will mostly govern how a cross border investigation will be conducted and ultimately, if there is an indictment and a trial, where and how the criminal trial will be undertaken.

The focus remains on ensuring that a client's right to a fair trial(s) is not prejudiced because of any irregularities in the area of data exchange, mutual assistance and potential breaches of fundamental human rights, such as the right to silence, across each jurisdiction where criminal and regulatory exposure exists. Having access to up to date local knowledge concerning which Government lawyers will be taking on the case, profiling the appetite of the particular prosecution team to try and resolve the matter through a negotiated plea/settlement/DPA and making the key forensic decisions very early on about your client's potential value to the Prosecution are some additional challenges that arise in cross border investigations. It is advisable to work collaboratively with experienced lawyers in all the jurisdictions where your client may be facing criminal and regulatory exposure to navigate some of these challenges.

Krys: Given the nature of offshore fraud/crime, almost all of it is of a cross-border nature. Neither the fraudster, victim, documents, or assets will usually be found offshore. Knowing where to find and then obtain access to information and assets is always the primary objective of the fraud investigator. Failing to being able to do this can also be the greatest obstacle to a successful prosecution.

Accordingly having a good sense of the various remedies available globally to collect evidence and information is critical. When we assess the alternatives available to us, we will look at the competence of the legal profession, the appetite of the courts to take on complex issues, the integrity and transparency of the court process, the efficiency of getting a decision and the willingness of the court to makes parties accountable when orders are issued.

Having a well-considered legal strategy is also important. Too often we see litigation strategies by other groups started prematurely before appropriate evidence is collected or pursued in a multi-faceted context that is easily struck out in the early stages. Funding can be an issue in some instances, particularly in the early stages of investigations, as many litigation funders are unwilling to provide funds without a legal opinion in hand.

Furthermore, with the growing number of jurisdictions implementing more stringent data privacy laws which introduce a variety of challenges in the collection, review, and production of data offshore, it is imperative that we engage expertise in cross-border eDiscovery management earlier rather than later. Regulations may affect from whom and what data may be collected, and where that data may be reviewed. One may be subjected to steep fines and crippling sanctions for even the innocent violation of such regulations and court rules. With the General Data Protection Regulations (GDPR) going into effect in 2018, and many offshore jurisdictions enacting similar initiatives, compliance may appear to be a daunting task, but it is undoubtedly a necessary one.

Angotti: (i) Cross Border Challenges

As an initial matter, cooperation among foreign law enforcement agencies has steadily increased over the last five years. For some jurisdictions, the quality of cooperation has improved to levels of collaboration, with active joint investigations beyond information sharing. This has enabled the DOJ to more easily obtain evidence overseas and to resolve cross-border investigations of transnational criminals. The expansion of FBI and DOJ international corruption targeting capabilities has also benefitted from cross border collaboration.[1]

Government investigators have improved their ability to collectively work through Mutual Legal Assistance Treaties and extradition arrangements in joint pursuit of criminals. The facilities provided by Interpol to share intelligence and contacts also promotes international cooperation.

There are still significant challenges to cross-border investigations. Governments need to more quickly establish cross-border jurisdictional authority to pursue investigations, develop stronger intergovernmental relationships to elicit cooperation and provide easier access to witnesses and evidence to law enforcement authorities in other jurisdictions.

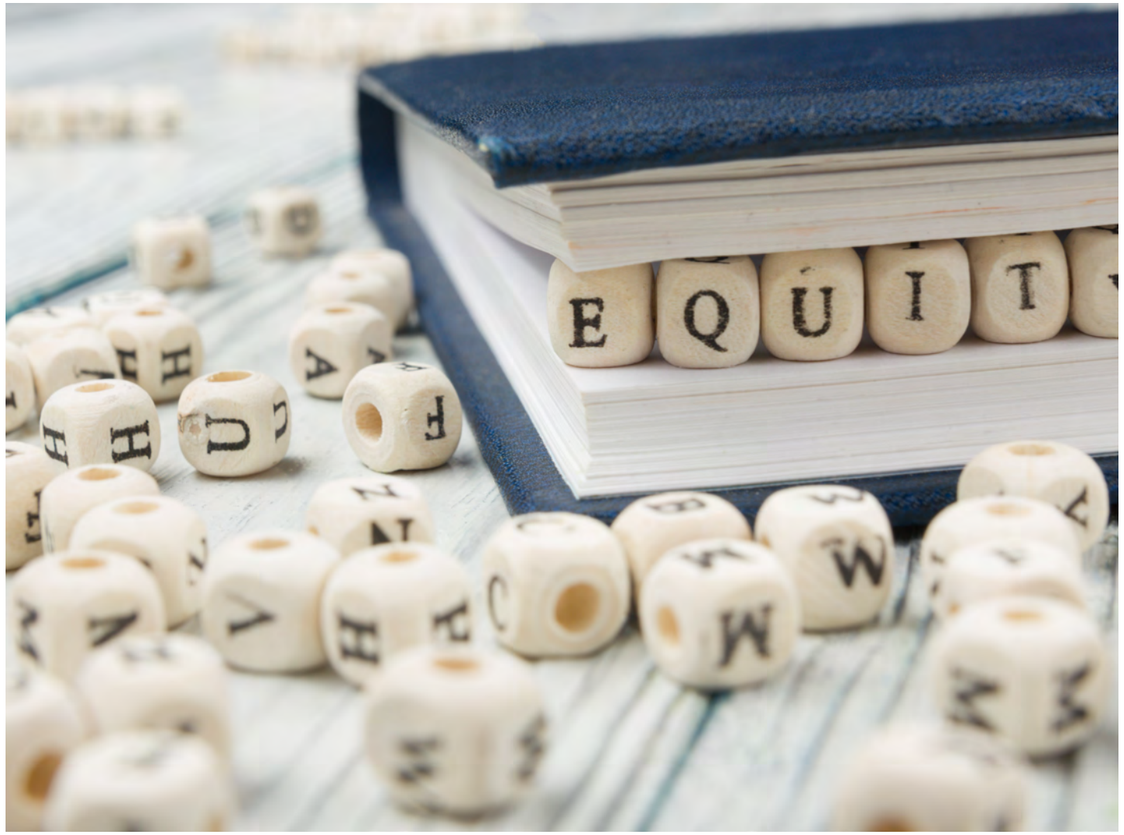
(ii) Data Privacy

Data privacy challenges, including data protection laws and regulations, employment law, local legislation, etc. can constrain cross-border cooperation. These challenges can exist even when a company under investigation chooses to cooperate with an investigation. The European Union General Data Protection Regulation ("GDPR") has created key areas to be noted when encountering and managing data related to EU member countries. They include:[2]

- Increased Territorial Scope making it applicable to all companies processing the personal data of subjects residing in the EU.
- Penalties for being in breach of GDPR requirements.
- Requirement that requests for consent to data owners be given in an intelligible and easily accessible form, making it as easy to withdraw consent as to give it.

1. FBI.gov website, Public Corruption - https://www.fbi.gov/investigate/public-corruption

2. EUGDPR.org - https://www.eugdpr.org/



Many countries are implementing regulations similar to the GDPR. It will be essential for investigating agencies to ensure compliance with this myriad of international data privacy statues and regulations to protect the rights of witnesses and targets, and the integrity of the investigations.

Data Privacy laws in some countries make it more difficult for law firms and investigators to comply with the Yates memo, which seeks to hold individuals accountable for illegal corporate conduct and provide corporations credit for providing information to the DOJ about individual culpability.[3] For example, some jurisdictions require the names of employees and former employees to be redacted from documents prior to being produced to US authorities. This may impact the ability of government investigators to charge culpable individuals in corporate investigations.

(iii) Cross Border Investigations Awareness

Private and public sector investigators conducting cross-border investigations should, before commencing an investigation, conduct due diligence on the country, develop contacts in the country, and educate themselves on local laws that might restrict contacts with witnesses and other individuals of interest, or the acquisition and transfer of evidentiary information. Failure to make the proper contacts and comply with local laws can subject investigators to penalties such as expulsion or prosecution.

3. Deputy Attorney General Memorandum, Individual Accountability for Corporate Wrongdoing, September 9, 2015 - https://www.justice.gov/archives/dag/file/769036/download

7. What are the main benefits and drawbacks of a DPA [Deferred Prosecution Agreement] scheme?

Uscov: Romania has not ratified OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions and, unfortunately, it has not adopted any form of DPA for other offences, despite the main benefits on long term which are presented in the OECD reports.
In Romania, the only form of agreement between a prosecutor and the defendant is the plea bargain, which is still not frequently used in fraud and white collar crimes due to the hesitation of prosecutors in using such efficient instrument.

The plea bargain may only be concluded with respect to offences punishable by fine or imprisonment for a maximum of 15 years and it is concluded when, from the evidence adduced, there is sufficient evidence of the existence of the offense and the guilt of the defendant.

The defendant benefits from the reduction by one third of the limits of the punishment provided by the law in the case of the prison sentence and the reduction by one fourth of the penalty limits provided by the law in the case of the penalty of the fine.

After the plea bargain is concluded, the court will rule on its admission or rejection.

Stetter: German law does not provide the legal framework for Deferred Prosecution Agreements that would be, neither in nature nor extent, comparable to the practise in the United States.

Markel: The key benefit is that it allows a company and its officers to avoid a criminal conviction. It also gives formal recognition and credit for actions the organisation has taken to remedy the issues or wrongdoing that led to it being under investigation.

Some believe that DPAs may not act as a deterrent for misconduct. Instead, they claim, that companies can pay a financial penalty and avoid more serious consequences. However in many instances, the terms of the DPA calls for the appointment of a monitor or an independent consultant which essentially adds to the cost of the settlement – this is generally imposed to provide the government with comfort that the company's internal control system will be assessed and enhanced to ensure compliance with the laws. While an added cost, if approached with the appropriate mind set, enhancements can lead to benefits that far exceed the costs. For example, weak controls may have allowed for employee embezzlements, kickbacks, or other schemes that steal from the company's bottom line.

Controls improved through investment in a monitor can identify these instances at an earlier stage or prevent them altogether. Governments need to recognise that the pursuit of profits is appropriate. And both the company and the government need to push to ensure the goal of "Clean Earnings" – or in other words, making the money in a manner in which the company gets to keep it.

Angotti: Between 2002 and 2016, the U.S. DOJ entered into more than 400 DPAs, and in 2016 the U.S. Securities and Exchange Commission (SEC) announced its first ever DPA with an individual in an FCPA case.[1] The increased use and reliance on DPAs has spread to other jurisdictions as well. The UK's Serious Fraud Office ("SFO") entered its first DPA with Standard Bank in November 2015 and France entered into its first DPA with HSBC in November 2017 under its new anti-corruption law, Sapin II.[2]

Benefits

- Avoidance of Criminal Conviction / Proceedings: DPAs enable the government to hold a company accountable for criminal conduct, require meaningful remediation, forfeit profits attained through criminal activity. In exchange, the company avoids potential indictments with collateral consequences that may harm innocent employees.

- Incentives for Self-Reporting: DPAs provide the prospect of a favourable settlement and therefore can incentivise self-reporting violations and co-operation with investigations.

- Compliance Programs, Monitorships, and Flexibility: Deferred prosecutions can require a company to revamp its compliance programs worldwide, and require periodic reporting to the government to track compliance. A DPA provides law enforcement with an ability to tailor compliance improvement requirements specifically to the entity.[3]

Drawbacks

- There has been much criticism of DPAs over the past few years. For example. Judge Jed Rakoff wrote that most DPAs, while often obscuring who was personally responsible for the company's misconduct, fail to achieve meaningful structural or ethical reform within the company itself. The recommendation is instead that various steps be taken to improve their efficacy, including greater judicial oversight, greater use of court-appointed monitors, and greater attention to breaches of the agreements.[4]

- Does it Deter Corporate Wrongdoing? There are differing opinions on the effectiveness of DPAs, but critics often point to firms that pay a fine, pledge to change, and return to the same behaviour. Pfizer has been the subject of three DPAs for illegal marketing, bribing doctors, and other crimes. Other critics have pointed to the light financial sanctions applied to some perpetrators, for example most recently the £497.25 million DPA offered to Rolls-Royce in the UK in February 2017.[5]

- Intrusion into Corporate Governance: Some critics have concerns that DPAs invite an unhealthy degree of prosecutorial intrusion. With deferred prosecutions, prosecutors may be tempted to interfere into corporate governance matters as the government's or the monitor's daily presence may impact a company's business development and stock price.[6]

1. https://www.newyorker.com/magazine/2017/07/31/why-corrupt-bankers-; http://masonlec.org/site/rte; https://www.sec.gov/news/press-release/2013-241

2. https://www.sfo.gov.uk/2015/11/30/sfo-agrees-first-uk-dpa-with-standard-bank/; http://www.fcpablog.com/blog/2017/11/28/france-enforcement-hsbc-pays-300-million-for-first-dpa.html

3. https://www.forbes.com/sites/insider/2015/05/28/deferred-prosecution-agreements-the-going-gets-tougher/2/#64cf9dff53ac

4. Justice Deferred is Justice Denied, U.S. District Court Judge Jed S. Rakoff, February 19, 2015 – http://www.nybooks.com/articles/2015/02/19/justice-deferred-justice-denied/

5. http://www.mondaq.com/unitedstates/x/570370/Corporate+Crime/Lessons+Learned+From+The+RollsRoyce+Deferred

6. http://www.hastingslawjournal.org/wp-content/uploads/Golumbic-Lichy-65.5.pdf

8. To what extent has a changing technological landscape and professionalisation of cyber criminals altered the way in which information security is delivered?

Uscov: Artificial intelligence has an unprecedented development, so the planned changes primarily target the security area.

On the one hand, the security of discoveries must be ensured both in the research phase and after their registration with the competent bodies (especially with regard to inventions falling under the scope of national security and whose disclosure is limited).

On the other hand, it is important to consider securing data connections for inventions based on artificial intelligence so that they are not hacked and used for purposes other than those for which they were thought.

Last but not least, given that AI can acquire a mode of action that imitates human behaviour – with the only difference of lack of discernment in the case of AI – in the case of AI committing an offence, the guilty human being must be identified. This approach may be difficult in the context of AIs being able to come into contact with multiple people, the AI's illicit behaviour may be a mix of learned behaviours but each one does not constitute illicit behaviour or AI can process human being behaviour in a way different from the way it was transmitted by the human being.

Technical solutions that are implemented to prevent cybercriminals need to be duplicated by adapted legal solutions. As far as cybercrime is concerned, it will have a development that, at least in part, we can anticipate at this time, but for which the international environment is not prepared at the legislative level. In this regard, let's take the example of cryptocurrencies that have been in a continuous development for many years, being both traded and used for the exchange of various products (improperly said "bought"), but for which in Romania, as an example, there are no regulations, while cryptocurrencies may come from or may be used in cybercrime.

Sikellis: Traditionally, informational security consisted of internal protection measures, security awareness, on-demand consulting, and topic-specific auditing. While these functions are still necessary in the ever changing technological landscape, we must recognise that cyber criminals can circumvent traditional protective measures and exploit vulnerabilities due to the sophistication of their TTPs (Tactics, Techniques, and Procedures). No more is this apparent than in how common cyber criminals are currently utilising advanced malware that had been previously used only by state-funded threat actors.

To handle the current dynamic in cybercrime, we need to modernise our response teams and their technology. On the team side, we need cyber-savvy individuals with unique and sophisticated skill-sets to not only detect and respond to cyber threats, but also proactively hunt for and, hopefully, prevent them. But high-quality teams, by themselves, are not a remedy to all threat actors because the current rate and sophistication of the attacks are higher than ever before.

For cyber security teams to be successful, they need to quickly and thoroughly process massive amounts of data. Fundamentally, these teams are big data shops that use machine learning and artificial intelligence for their threat detections and event correlations. In Siemens, our cyber security infrastructure ingests billions of events per day in order to meet this need and it would be impossible for the teams to handle this data without the corresponding technology.

> *"Technology can not only assist with the collection and analysis of data but also when the information is collected, in storing it and putting it into a forum for easy and efficient retrieval and analysis."*
>
> *- Kenneth M. Krys*

Miralis: The increasing threat of cybercriminals has not been adequately addressed by Australia's domestic criminal law, which is generally not very effective in prosecuting international cybercriminals. It is well known that most of the sophisticated cyber-attacks originate outside of Australia's borders however such offenders are rarely investigated due to restrictions in obtaining evidence in foreign jurisdictions and lack of harmony in international law in the areas of mutual assistance and extradition which is essential for an effective response to the increased internationalisation of cybercrime.

This is a problem which appears to be universal despite the international conventions on cybercrime. Information security is therefore an increasingly important topic across all government and private sectors that have had to respond to these increased threats. The need for the private sector to take care of its own cyber security is being emphasised as the first line of defence. The Government however actively provides open source advice to the private sector about how to protect its information security and in 2017 created a Cyber Resilience Taskforce which is intended to engage broadly with the private sector, as well as Commonwealth, state and territory government agencies to bring forward the new ideas needed to build national cyber security capacity and capability.

While the primary focus of the Taskforce is on ensuring Australia responds effectively to cyber security threats and incidents, it will also be used as opportunity to explore related areas around communications, governance and partnerships across government and industry to present a multidimensional national cyber resilience model.

Krys: Forensic technology is an important tool in the arsenal of services we provide clients. Clients expect fraud investigators to have technology specialists on the strategic team. Technology can not only assist with the collection and analysis of data but also when the information is collected, in storing it and putting it into a forum for easy and efficient retrieval and analysis. We are constantly refreshing and updating our technology capabilities. With regard to cyber-crime, there have been three impacts of this: (i) With the recent offshore hacks, we are more vigilant in making sure the information we collect is secure and maintained to the highest of standards; (ii) Clients who share information with us are more frequently seeking assurance regarding the systems we have in place to protect their information; and, (iii) We can assist those clients who want their systems tested with a cyber-audit.

Angotti: (i) Changing Technological Landscape

The challenge, as the technology landscape changes, is that business must anticipate and react to the latest cyber hacking threats through selection, acquisition and implementation of relevant and updated hardware and software to defend against internal and external attacks. In addition, businesses must defend against penetration from all points.

Bad actors create the latest threats and merely have to use existing or newly created penetration techniques to breach new technology at any given point to be successful. Techniques for attack include: malware, phishing, SQL injection, cross-site scripting, denial of service, session hijacking, man in the middle, credential reuse, and business email compromise. [1]

Another significant risk for business is created by the Internet of Things ("IoT"), which is tying in devices and infrastructure not originally intended for internet access. The advent of IoT creates challenges for maintaining confidentiality, vulnerability in its connectivity.[2] Many of these systems were not originally designed to protect personal data, which also may compromise privacy expectations. In addition, more devices connected to the internet means more opportunity for compromise and penetration, especially if the devices do not have appropriate encryption and firewall systems in place, and if consumers are not aware of the vulnerability.

(ii) Professionalisation of Cyber Criminals

According to Interpol, "cybercrime has matured to become a business sector driven by consumer demand..."[3] The dark web is a marketplace constructed to provide "services" to "consumers" looking to conduct bad acts, from enabling the purchase of illegal drugs (opioids such as fentanyl and heroin) and other illegal contraband to facilitating the sale of software to conduct malware attacks against an industry.

Payment for these illegal services and products is usually in the form of cryptocurrency such as Bitcoin, making the product purchase and movement of funds difficult to track.[4] That does not mean, however, it is untraceable, as it is likely the profiteers of this activity will in some cases follow traditional money laundering avenues.

(iii) Information Security Delivery

Technology and techniques for cyber-attacks available to bad actors can be more sophisticated than those used by businesses. Companies must understand the vulnerabilities of their technology and the risks created. They should then design their systems and processes to mitigate those risks with an organised process through designing a plan such as the 7 Pillars of Cyber Resilience.[5]

Companies and financial institutions should also consider working with a reputable digital forensics entity both before a breach to develop robust defences, and after a breach to mitigate the damage.

1. Common Types of Cybersecurity Attacks, RAPID7 - https://www.rapid7.com/fundamentals/types-of-attacks/

2. The "Internet of Things" at Risk, Gilles Hilary, INSEAD Professor of Accounting and Control, and Rudi Spaan, President and CEO AIG Hong Kong | December 9, 2015 - https://knowledge.insead.edu/blog/insead-blog/the-internet-of-things-at-risk-4406

3. The Professionalisation of Cyber Criminals, Gilles Hilary, INSEAD Professor of Accounting and Control and Christophe Durand, Head of Cyber Strategy, INTERPOL | April 11, 2016 - https://knowledge.insead.edu/blog/insead-blog/the-professionalisation-of-cyber-criminals-4626

4. DHS works around the clock to track cyber crime on the "dark web", Jory Heckman, Federal News Radio, December 15, 2017 - https://federalnewsradio.com/dhs-15th-anniversary/2017/12/dhs-works-around-the-clock-to-track-cyber-crime-on-the-dark

5. CorporateLiveWire, Cyber Security 2017, Virtual Round Table - http://www.cugiacuomo.it/public/pubblicazioni/Cyber_Security

9. What measures can be implemented to help minimise risk following a security breach?

Sikellis: In the current cyber environment, risk is best understood in the context of WHEN a breach will occur, and not IF—indeed, to assume otherwise recklessly ignores the likelihood of such an attack and subjects companies to even greater risk. To fully understand and minimise this risk, three areas need to be explored: organisational readiness; vendor management; and customer contracts.

When evaluating organisational readiness, it is critical to identify a task force from members of a designated response team who will then critically analyse the adequacy of incident response (technical) and incident handling (management) processes. One of the goals is to identify touch-points and potential conflicts between the cyber security team and those handling corporate security, legal, procurement, data privacy, and customer contacts.

Vendor management (procurement) sometimes is overlooked in the cyber security context, but its implications for risk mitigation are critical, especially with respect to applications, software, and other IT outsourcing. Are your vendors really as committed to incident or breach response as your internal organisation? Do your vendors bring expertise that does not exist within your own staff? Is procurement an enabler of or inhibitor to the agility of your response? These questions all must be addressed in order to properly mitigate vendor-related risks.

The third area, customer contracts, has recently developed into a critical area of risk mitigation. As more businesses suffer a cyber attack, the data security industry is becoming more sophisticated and bolstering language in contracts to ensure proper protection. Indeed, companies often are not even aware that many of their Master Services Agreements already contain protective language. As the saying goes, it's better to repair the roof when it is sunny than during the rainstorm.

Krys: Of course the best remedy is prevention, and taking steps to avoid such a breach and knowing what data you hold should be a priority for all service providers. But if a security breach occurs, the following issues may arise: (i) loss of information, (ii) criminal/civil actions, and (iii) reputational risk. In order to minimise or mitigate the risks that face the service provider, the following should be considered. Contact the insurance company and notify them of the breach. You should also contact your attorneys and identify what remedies may be available. Depending on your knowledge of the breach and what if anything has been stolen, you may be able to injunct the data from being released into the public domain or take steps to protect the data. Lastly you will want to consider a public relations team, in order to inform customers of the breach and possible implications for them and deal with any publicity that might arise.

In addition to the legal and public relations steps outlined above, technological and counter cyber threat measures may be employed to both mitigate any resulting damages, and reduce future risks of exposure. Immediately (or as soon as the breach is discovered) identifying precisely what breaches may have occurred, such as password or personal information compromise, software vulnerabilities, and malicious code, is a criti-

> *"Once an alert of intrusion is raised, either by detection systems, anti-malware or personnel, specialised personnel should review the incident alert and determine whether it refers to a typical problem or an incident that needs to be escalated."*
>
> *- Alma Angotti*

cal first step, which allows an organisation to plug any holes that may exist in its network and data security policies. It also enables an organisation to investigate whether confidential information is being sold or distributed on the dark web.

Angotti: After detecting and verifying a security breach, organisations should:[1]

Investigate and assess: Once an alert of intrusion is raised, either by detection systems, anti-malware or personnel, specialised personnel should review the incident alert and determine whether it refers to a typical problem or an incident that needs to be escalated.

Contain the impact: Once the incident is escalated and confirmed as a security incident, the goal is to limit the effect of the incident.

Report the incident: When incidents involve sensitive data retained within the organisation's systems, organisations often have a legal requirement to report the incident externally. Organisations might also be required to notify the individuals affected by the incident and in some cases, official government agencies.

Recovery: (i) Restore or rebuild systems and data as needed. (ii) A major incident may require partially or fully rebuilding systems, and restoring all the data from the most recent back up. (iii) Review and identify unnecessary, inefficient or missing security services and protocols. (iv) Confirm access control lists (ACLs) are reviewed and updated. (v) Confirm that all up-to-date patches are installed, and that user accounts and their privileges are not set as default.

Remediation: (i) Perform a root cause analysis, examining all the elements of the system to determine what allowed the incident to happen. (ii) Recommend the changes needed to mitigate the vulnerability identified in the root cause analysis. (iii) Remediating steps could include, among others:

- Implementing a patch management program;
- Enhancing the Security and Incident Response program; or
- Enhancing elements of compliance programs.

Messaging: (i) Develop an internal and external communication plan ready to execute at the time of a breach. (ii) Coordinate with a professional public relations firm that has experiencing in dealing with breaches.

Lessons learned: Identify areas where incident response can be improved:

- Personnel might not have adequate training, knowledge or expertise to respond to incidents effectively;
- Some security controls were not previously tested or need to be updated; or
- Some procedures or protocols are not clearly understood or are outdated.

1. Official Study Guide for the Certified Information Systems Security Professional ("CISSP") certification, James M. Stewart, Mike Chapple, Darril Gibson

10. How can companies ensure they get the balance right between implementing risk management and risk prevention?

Sikellis: Risk management and risk prevention go hand-in-hand. You have to start with an enterprise-wide risk-monitoring system that is fully supported by the business from top to bottom, which then feeds into your daily work in risk prevention. This risk monitoring system must have "tentacles" in every aspect of the business, as well as in all of your compliance processes. For example, you have to continuously ask the right questions during your project assessment phases and carefully monitor your cases for trends and systemic concerns.

This also means you need a rigorous due-diligence process and related compliance checks for critical issues, such as anti-money laundering protocols and Human Rights concerns. Once you collect the risk data from these tentacles, the critical next step is to effectively use that information. Many compliance systems fail at this point: after successfully mitigating risks and handling compliance investigations, there is no proactive "lessons learned" efforts or other steps taken to prevent future similar risks. Indeed, those efforts serve to drive the much needed evolution of the risk prevention system so that it can keep up with the constantly changing technological landscape.

Krys: This is a tricky issue and one that I, as the Executive Chairman of a smaller firm, find myself having to address daily. The approach I take is to have sufficient information at my disposal so I that I can understand and monitor the risks my firm is facing. We have a business risk assessment paper for our firm that identifies our risks and assesses them to determine which areas we are vulnerable. Another thing we do is ensure the primary risk management is done upfront. For me, risk prevention is easier if you mitigate the risk at the beginning of the particular project or relationship and to the extent you have identified a risk, you are then monitoring it and assessing it on an on-going basis. We also have reporting mechanisms and compliance checks conducted on a pre-determined periodic basis to check we are taking the steps we identified up front and assessing the risk.

Ultimately what you are hoping to achieve is something that is manageable, effective and yet not such a burden that it drains your resources and checkbook.

Markel: Minimising fraud and white collar crime is best accomplished when the missions of corporations and governments are aligned. Both parties should recognise the importance of investing in internal controls – are they designed appropriately? Communicated and implemented effectively and monitored to identify deviations at an early stage? The company will need to make the investment – and governments should recognise the efforts undertaken and not expect perfection. From an enforcement perspective, governments should also be thoughtful in the scope of their inquiries and give credit to companies who are proactive in preventing fraud and responding to indications of fraud. While the U.S. Department of Justice appears to be making strides in this area based on new FCPA cooperation guidance that they released in November of 2017, it remains to be seen if the SEC will follow suit. Also, harmonisation of international laws and consistency in enforcement of those laws would allow for predictability and an appropriate allocation of resources by companies.

Angotti: (i) **Risk Management**
Effective risk management implies that senior management makes deliberate decisions to understand, accept and mitigate the risk. The risks change and organisations should have a consistent capability to identify new risks. This requires resources,[1] commitment and authority given to responsible individuals.

Once the risks are identified, companies can institute controls to help mitigate and manage the risk. These may include background screenings and in-depth investigations on third parties to control the risk of bribery and corruption by agents, and providing anti-fraud or other types of training to increase employee awareness of potentially regulatory pitfalls. It may also be increasing accountability for compliance across the organisation by including a compliance metric in performance evaluations and also mitigating risk of internal fraud and embezzlement by ensuring the segregation of duties, or exercising audit rights.

Communicating the risk strategy broadly, collaborating between all departments of an organisation, and identifying and reporting on emerging risks are essential for understanding the risks and accurately disseminating the information to relevant stakeholders to be able to manage these risks.

(ii) **Risk Prevention**
Risk prevention means the act or practice of stopping something bad from happening.[2] Risk prevention methods include all techniques and management practices that help to avoid unnecessary or foreseeable risks and establishes threat and vulnerability mitigating countermeasures. Each organisation should tailor relevant industry best practices risk prevention methods to fit its needs. This may include limiting the products it offers or geographies in which it is willing to do business. It might include deciding not to accept certain types of clients.

(iii) Risk Balance
Companies can ensure the right balance between risk management and risk prevention by identifying risks and determining how much risk they are willing to tolerate. Senior management must set its risk appetite based on a careful analysis of various factors, including the following:

- Regulatory impact.
- Consumer impact.
- Reputational impact.
- Existence of an enforcement action, i.e. consent order, DPA, etc.
- Financial reward impact.

Senior management can then manage the risk by either eliminating it, by exiting certain customers for example, or by managing it by ensuring an adequate control environment. Risk management and risk prevention share the same goal, to reduce the organisation's risk, loss and liability exposure. [3]

1. https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management/risk

2. https://oshwiki.eu/wiki/Prevention_and_control_strategies

3. http://coanet.org/standard/rpm/

11. In an ideal world what would you like to see implemented or changed?

Stetter: In Germany, the effects of the discussed crimes are very serious (e.g. disgorgement) for both private and legal persons even though Germany does not dispose of a corporate criminal law. In an ideal world, the companies would be able to formulate their internal codes of conducts on the basis of clear regulations to make sure employees easily find and understand the line between criminal and unpunishable behaviour. The current legal regulations do not provide for such a clear line which in practise is leading to frequent difficulties in understanding and implementation. Just to avoid any form of risk, companies are de facto forced to implement general interdictions.

Miralis: As the internationalisation of white collar crime continues apace, unprecedented cooperation between regulators and law enforcement bodies will exponentially increase in the areas of tax fraud, cyber fraud, foreign bribery, bitcoin investigations and money laundering. The legal mechanism which will give effect to this cooperation will include mutual assistance, Memorandums Of Understanding, and informal contact between financial regulators and law enforcement with their partner agencies across the globe. These developments are necessary to properly deal with the complexities of a globalised world where the nature of de regulated markets and the fluidity of capital through the internet has eroded the concept of national crime.

Often, however, much of what is occurring in this space is not sufficiently subjected to the necessary regulatory and or judicial oversight required. Given that these developments have the capacity to interfere with the protection of fundamental rights, I would like to see a clearer framework developed that strikes the right balance between the need for appropriate powers to be provided to Governments and the protection of important rights such as the right to an a fair trial and the right to silence.

Angotti: (i) Ensure Compliance Officers have appropriate executive and Board access and authority and resources to protect the company. (ii) Continue enforcement of effective anti-fraud laws that include but are not limited to the FCPA, export controls, economic sanctions, AML, Cybersecurity and financial fraud. (iii) Expand information sharing between government and financial institutions, so that financial institutions can maximise their assistance to law enforcement by targeting known criminal typologies. (iv) Expand avenues for information sharing and investigative cooperation between foreign governments through treaties and agile international task forces concerning criminal threats. (v) Countries should continue to enhance and augment their current anti-fraud and financial legislation, striving to develop and establish AML and CTF regimes that will allow them to effectively investigate and prosecute criminals. (vi) Establish and strengthen laws to prevent abuse of corporate forms, obscuring the proceeds of crime.