IADC COMMITTEE NEWSLETTER

INTERNATIONAL

MAY 2015

IN THIS ISSUE

Cyber Security: Be Selfish and take care of yourself! Cyber Security has been a focus for International Law Firms for some time. But while they work to help their clients, is it time now to make sure their own systems are properly structured to avoid breaches?

Cyber Security for International Lawyers

ABOUT THE AUTHORS

Bob Craig brings 40 years of legal experience to advise clients in identifying and selecting consulting and testifying experts for litigation. Mr. Craig brings strategic, tactical, and practical experience to his work. Specifically, he has an extensive background in all types of litigation matters, ranging from major securities cases and significant international arbitrations to industry-wide antitrust actions and critical intellectual property cases. He also has been retained personally as a court-designated independent in derivative litigation and is available for arbitration and mediation appointments. He can be reached at bcraig@thinkbrg.com.

Norman Comstock advises clients on enterprise risk management, information technology governance, technology assurance, program management, and cybersecurity. Mr. Comstock has experience leading complex, high-profile projects and initiatives for investment due diligence, integration, divestitures, and program management for high-risk, multiyear, multi-vendor projects. He has advised clients across diverse industries and geographies including construction, energy, financial services, healthcare, higher education, high technology, and manufacturing, as well as state, local, and federal governments. He can be reached at ncomstock@thinkbrg.com.

ABOUT THE COMMITTEE

The International Committee is the core international group in IADC and serves those members who have an interest in transnational or international legal matters including transactions, litigation, and arbitration. Thus any member, whether in the USA or abroad, who does cases with a foreign element (inbound or outbound) will find involvement in this committee extremely useful. Many of the members of the committee are from outside the USA, and this provides a rich mix of experiences and expertise as well as great networking opportunities. The International Committee also organizes European Regional Meetings and contributes to the International Corporate Counsel College. Learn more about the Committee at www.iadclaw.org. To contribute a newsletter article, contact:

Peter Pliszka
Vice Chair of Newsletters
Fasken Martineau DuMoulin LLP
ppliszka@fasken.com

Introduction

Worries about cyber security threats have been high on the docket of concerns for International practitioners for some time. And much has been done to address these issues. For instance, the Tallinn Manual, first issued in 2009, has as its vision to "be the main source of expertise in the field of cooperative cyber defence by accumulating, creating, and disseminating knowledge in related matters within NATO, NATO nations and partners."[1] Cyber attacks, cyber security and even cyber warfare have become well known terms in the International arena – and more importantly, real world issues. No International Law Firm or lawyer practicing internationally can say that cyber issues haven't played out in practice, at least as a concern to be reckoned with.

But the major focus for many lawyers has been on the task of arming clients to guard against cyber issues and addressing breaches when they occur to clients. Perhaps in the dedication to the clients, however, care to assure firms, even sole-practitioner firms, are themselves adequately guarding their own 'house' has been a process too often left unattended.

The lifecycle of many client matters flows through international law firms. Company formation, capital structure, patents, trade secrets, mergers, acquisitions, divestitures, intellectual property rights, and employee contracts are just some of the areas of legal advice undertaken by firms, not to mention the sensitive information that is exchanged as a result of litigation. Cyber threat actors know this too. The growth of cyber threats portends a number of challenges for the International Lawyer. As the world has become more digital and connected by the Internet, so have law firms. As such, the waves of cyber threats targeting the digital assets of financial targets, critical infrastructure, intellectual property, and sensitive data have increased exponentially wherever it can be discovered and profited from.[2]

First, consider how the phone has emerged from a single-use communication tool to a 'smart' hand-held computer with emerging and multiplying uses and risks. Consumerism has quickly accepted waves of new phone technologies that have transformed individual and group productivity and efficiency. In fact, ubiquitous mobile device adoption and game-changing economies of scale evolving from cloud computing have blurred the lines between personal and business usage. As a result, many organizations have adopted Bring Your Own Device (aka BYOD policies).[3] While this has presented some welcome corporate procurement and maintenance expense savings it has also surfaced many unintended consequences, particularly, security vulnerabilities that provides pathways for viruses and malware to spread laterally across law firm networks. Never

[1] https://ccdcoe.org/tallinn-manual-0.html

[2] http://www.pewinternet.org/files/2014/10/PI_FutureofCyberattacks_102914_pdf.pdf

[3] http://www.cisco.com/web/about/ac79/docs/re/BYOD_Horizons-Global.pdf

forget the primary objective of cyber criminals is to exfiltrate sensitive data.

With more devices, in addition to what used to be a common phone, available in the worldwide, Internet-connected environment, the potential for compromised devices of all kinds to become assimilated into a growing bot-net army is unprecedented. Who are the good guys and the bad guys in the digital world? Law enforcement, along with the public and private sector, has been struggling to understand who the cyber attackers are. There are "hacktivist" groups like Anonymous[4], who claim responsibility for their exploits, but many hackers choose never to identify themselves and use sophisticated techniques to avoid detection. The cyber criminals' creativity, persistence, and patience coupled with the breadth and pace of vulnerability information sharing makes cyber security an insidious problem for companies and individuals, including law firms and lawyers, many of whom feel that they lack the resources to effectively defend themselves. Without simplifying the issues too greatly, however, there is practical guidance to prevent data loss, detect unauthorized usage, and correct vulnerabilities from future exploitation.

Like any other organization, international law firms have finite resources and inherent risks. Five key considerations to help manage cyber threats are IT Governance, Data Classification, User Awareness Training, Independent Assessment, and Incident Response Teams.

IT Governance

IT Governance is a key discipline to identify IT related needs, organization capabilities and risk management requirements. ISACA International first published its authoritative IT Governance framework, Control Objectives for Information Technology (COBIT) in 1996. The latest version, COBIT 5, was published in 2012[5] and has been instrumental in guiding organizations of all sizes and from many industries to align IT with the business objectives. COBIT 5 is comprehensive and addresses five principles:

1. Meeting Stakeholder Needs – and for this the stakeholder is both the lawyer and the client.
2. Cover the Enterprise End-to-End
3. Apply a single integrated framework
4. Enable a holistic approach
5. Separate governance from management

All of these principles are important, but the fifth principle is particularly key because it requires a structure for transparency and accountability. Many law firms may have a governance committee to address the firm's current and emerging issues. A primary take away is to have a good framework to help guide the governance committee to navigate IT operational risks. COBIT 5 covers 37 processes and provides a method to assess the capability maturity of the organization to manage those processes. A rigorous

[4] http://www.wired.com/2012/07/ff_anonymous/all/

[5] http://www.isaca.org/cobit/pages/default.aspx

assessment of these 37 areas will likely pinpoint areas that need attention either because the process is not done, the capabilities are under resourced, or the technologies are inadequate or no longer supported.

Table 1 - Cobit 5 an IT Governance Framework[6]

Governance **Evaluate, Direct and Monitor**
EDM01 Ensure Governance Framework Setting and Maintenance
EDM02 Ensure Benefits Delivery
EDM03 Ensure Risk Optimisation
EDM04 Ensure Resource Optimisation
EDM05 Ensure Stakeholder Transparency
Management **Align, Plan and Organise**
APO01 Manage the IT Management Framework
APO02 Manage Strategy
APO03 Manage Enterprise Architecture
APO04 Manage Innovation
APO05 Manage Portfolio
APO06 Manage Budget and Costs
APO07 Manage Human Resources
APO08 Manage Relationships
APO09 Manage Service Agreements
APO10 Manage Suppliers

[6] http://www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security
Build, Acquire and Operate
BAI01 Manage Programmes and Projects
BAI02 Manage Requirements Definition
BAI03 Manage Solutions Identification and Build
BAI04 Manage Availability and Capacity
BAI05 Manage Organisational Change Enablement
BAI06 Manage Changes
BAI07 Manage Change Acceptance and Transitioning
BAI08 Manage Knowledge
BAI09 Manage Assets
BAI10 Manage Configuration
Deliver, Service and Support
DSS01 Manage Operations
DSS02 Manage Service Requests and Incidents
DSS03 Manage Problems
DSS04 Manage Continuity
DSS05 Manage Security Services
DSS06 Manage Business Process Controls
Monitor, Evaluate and Assess
MEA01 Monitor, Evaluate and Assess Performance and Conformance
MEA02 Monitor, Evaluate and Assess the System of Internal Control
MEA03 Monitor, Evaluate and Assess Compliance with External Requirements

The governance committee can utilize this framework to assess process importance, performance, formality, and accountability. For example, APO10 Manage Suppliers is an important process for law firms that may rely heavily on third party service providers – such as for network managed services, help desk support, application support, log monitoring, etc. The framework becomes granular to guide the organization to consider these control objectives:

"**APO10.01 Identify and evaluate supplier relationships and contracts.** Identify suppliers and associated contracts and categorise them into type, significance and criticality. Establish supplier and contract evaluation criteria and evaluate the overall portfolio of existing and alternative suppliers and contracts.

APO10.02 Select suppliers. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimised with input from potential suppliers.

APO10.03 Manage supplier relationships and contracts. Formalise and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.

APO10.04 Manage supplier risk. Identify and manage risk relating to suppliers' ability to continually provide secure, efficient and effective service delivery.

APO10.05 Monitor supplier performance and compliance. Periodically review the overall performance of suppliers, compliance to contract requirements, and value for money, and address identified issues."

The framework is a good start but requires tailoring to the law firm. For example, in APO10.04, by supplier, it may be important to require that your managed services provider apply all system patches within one month of release and provide a business impact assessment for any patches that cannot be done in that time period (e.g. system instability or extended outage).

Data Classification

Document management systems have been in place for law firms for years, and many firms have focused their IT skill-set on making sure that the firm members are able to easily and efficiently access their documents to assure prompt and effective communication to the client. Most firms use these systems, either off –the-shelf, customized or by careful rules for their word-processing activities. As a part of these systems, data becomes identified and classified by code or descriptive note or similar technique. But Data Classification can be, and is, an Achilles heel for many organizations. There are many examples of private sector data classification standards that have been derived from ISO 27001 and public sector guidance like NIST 800-60 or

FIPS 199[7]; however, the challenge is having all partners and associates understand and practice the standards all the time. Moving from the paper analog world to the digital world has proved to be equally challenging. Therein lies the problem. It is common practice to transfer, process, and store much information (structured and unstructured data, files, images) with clients and associates across the globe; however workflows may not adequately prompt for classification, validate that it is classified correctly, or manage the data based on the specified policies effectively across all the nodes that it may traverse or come to rest. Rather, the emphasis at many firms has been ease of use over protection of data.

Encryption can be an effective risk mitigation technique but is not a panacea as it may not be available across all devices, locations, or networks. Of late, transport encryption methods have been discovered to be vulnerable and quickly exploited.

- Heartbleed,[8] April 204: a flaw in the open source OpenSSL cryptographic library affecting VPNs, webservers, and mobile devices.
- POODLE[9], October 2014: Vulnerability in the SSL 3.0 cryptographic protocol that could enable an attacker to access and read encrypted communications.
- FREAK[10], March 2015: Factoring attack on RSA-EXPORT Keys that downgrades encryption strength for browsers on Apple and Google devices when visiting various websites.

With this in mind, it is strongly recommended to gain an understanding of the firm-wide encryption strategy for data at rest, being processed, or transmitted. If there are any known vulnerabilities for those in use, get advice on the cost/benefit of stronger encryption alternatives.

User Awareness Training

The need for User Awareness Training is evergreen. The technology landscape changes, consumer choices change, user behaviors change. Existing employees and new employees all need ongoing security awareness training. User fatigue and user trust are two of the key issues. Users tire of the hype cycle around security issues; they become numb to the risk, especially if they have no first-hand experience. Employees are online longer, being exposed to "drive-by downloads" on websites. They trust the "friendly fire" emails forwarded from co-workers, friends, and family that beg them to open, read, and click on links. and Sophisticated hackers are crafting more authentic email, voicemail, and text

[7] http://www.iso.org/iso/home/standards/management-standards/iso27001.htm
[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0160
[9] http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-3566
[10] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2015-0204

messages using social network discovery, stolen email addresses or user credentials.

Consider supplementing your program with an active phishing campaign periodically if your user awareness program is a tired PowerPoint deck or a policy acknowledgment done once a year or only during employee onboarding. According to the Anti-Phishing Work Group 2Q 2014 report[11], the top countries hosting phishing sites were in the US, China, Germany, Turkey, Russian Federation, United Kingdom, France, Netherlands, Poland, and Canada. It is relatively easy to put a phishing email in front of everyone on your system to see which users are too quick to put the firm at risk. You're internal or external IT experts can likely handle this chore, or it is relatively inexpensive to outsource this kind of system test.

Independent Assessment

Independent Assessment is a critical governance tool to provide a comprehensive evaluation of implemented security policies, procedures, controls and staff in relation to best practices and industry standards. One of the critical components of this effort is to scan the network for potential vulnerabilities that can result in a large exposure. Going back to IT Governance, it's a good practice to separate governance from management. This is particularly important if your firm relies on external managed service providers to manage and maintain your network and systems. Vulnerability scanning services are relatively inexpensive. When vulnerability assessment results are interpreted appropriately by the service provider, the report can become a prioritized roadmap to efficiently address critical risks. It can also be a barometer for adherence to assessing vendor service level agreement. For instance, many vulnerabilities are fixed by regularly applying the patches provided by the vendors for the operating systems, applications, and devices in the environment. When old vulnerabilities exist (older than a year) or persist after a subsequent vulnerability scan, it may be because the managed services provider or IT department is under resourced, lacks capabilities, or is concerned with performance or availability issues of legacy systems. The IT Governance function should work with the independent assessor to validate the root cause. Nonetheless, it is imperative for international law firms to baseline and understand the expected assets, wireless access, ports, and network activity due to the use of BYOD devices and interactions with client traffic that may originate from the top phishing countries where you do not expect to have activity.

A more thorough and expensive test of the environment which also demonstrates the importance of training and hardware control, is to undertake a 'penetration test' performed by a third party. This entails hiring, essentially, a professional to 'hack' into your environment from any number of

[11] http://docs.apwg.org/reports/apwg_trends_report_q2_2014.pdf

ways that a real attacker might. Penetration testing has the benefits of testing your system security, identifying weaknesses in that security and identifying fixes where necessary. Additionally, the story of a penetration test is a highly effective tool in the training process.

Incident Response Planning

Provisioning an incident response team is an important prevention, detection, and correction planning step. Planning incident response when an incident is occurring is rarely neither productive nor successful. Realize that incident response involves a coordinated communication plan and orchestration of internal and external resources.

1. Put in place a trained team to monitor unusual behavior on the company's systems. Having the capabilities and wherewithal to adequately execute defensive strategies pales in comparison to the investment needed to field offensive strategies. Third party services for monitoring can be acquired as remote service and incident response digital forensics and e-Discovery need to be retained so they are available when necessary.
2. Prepare to manage the business impact of an attack on customers, suppliers and operations. Incident response is not the sole domain of security professionals. Rather, it is an exercise in communication to preparedness. International law firms may need to evaluate whether there is a need to update business continuity plans and testing procedures to ensure the firm can sustain a cyber-campaign.
3. Evaluate available countermeasures in terms of viability and effectiveness. Vulnerability assessments and Penetration testing are the normal tools to assess the defensive posture of a company's security environment. Testing that countermeasures are effective requires more time, energy, and realistic conditions. Disaster recovery techniques identify recovery time objectives to ascertain benchmarks for how long an organization's systems can be down without negatively impacting the business.
4. Establish relationships with international, federal and state cyber security officials. International law firms that perceive great cyber security risk should establish relationships with Europol, Interpol, and other international law enforcement agencies, as well as state law enforcement as well as federal agencies such as the Department of Homeland Security (DHS), and US Computer Emergency

Readiness Team (US-CERT)[12]. Sharing information about unusual network activity, denial of service attacks, phishing attacks, and quarantined malware provide more parties to be vigilant and coordinate observation of similar malicious activity which may help triangulate the identity of hackers.

5. Develop partnerships with key security vendors and systems/communications providers. Understand the technology roadmaps of the key security vendors and systems/communications providers. Opening up a dialogue with those vendors can help identify needs for security patches and co-opt there attention to unusual activity.
6. Assure there is an incident response review process. Spending time to understand lessons learned will help to improve future response activities.

Eligibility of firms for retention – Cyber Security takes hold

A final note about law services procurement issues in the United States and internationally that may or may not be obvious to the international practitioner. Whereas the tradition in the United States and internationally has been to hire both domestic and international counsel through law department contacts within the prospective client, a new trend is developing where a relationship with procurement, including a master service agreement and preliminary standards for retention, is becoming more and more common. In part this is driven by cyber security issues. Banks, particularly, are front-runners in this required pre-requisite to retention, and most have decided that the same level of cyber security required of them must now be required from their vendors. It is inevitable that cyber security will become a lynch-pin issue in the relationship between corporate clients and their firm, and a failure to be moving toward a more secure law office environment is now raising the potential that clients will be lost. Taking the steps to properly assure a strong cyber culture and environment is not only critical to the risk as it exists, but could be critical to the continued fortunes of the firm.

[12] https://www.europol.europa.eu
http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime
http://www.dhs.gov/topic/cybersecurity
https://www.us-cert.gov/

Past Committee Newsletters

Visit the Committee's newsletter archive online at www.iadclaw.org to read other articles published by the Committee. Prior articles include:

FEBRUARY 2015
A Commentary on the United Kingdom's Reappraisal of the Law as it Relates to Insurance Contracts
David Wilkinson

JANUARY 2015
A Review of Forum Non Conveniens in the United States and the Factors in Deciding Whether to Pursue an FNC Dismissal
Barry Davis

OCTOBER 2014
Litigation Funding in Australia - A Proposal for Reform
Stuart Clark

JUNE 2014
France and Belgium Adopt Class Actions Spring 2014
Christopher Scott D'Angelo and Jennifer Canfield

MAY 2014
Lago Agrio-Transnational Enforcement of Judgments
Be-Nazeer Damji

MARCH 2014
Pension Plans and Class Actions: The *Vivendi* Case
Louis Charette, Josée Dumoulin, Bernard Larocque and François Parent

FEBRUARY 2014
Canadian Price-Fixing Class Actions: The Supreme Court of Canada Gives the Green Light to Indirect Purchaser Claims
Steven F. Rosenhek and Vaso Maric

JULY 2013
Is The Class Action 'Centre of Gravity' Moving Away From the United States?
S. Stuart Clark, Ross McInnes, Colin Loveday. Andrew Morrison and Greg Williams

JUNE 2013
Australia's Poor Implementation and Enforcement of Anti-Bribery and Anti-Corruption Obligations – Change is Critical
Annette Hughes and Adam Purton

MAY 2013
Insurance Law Principles Influence the Court's Approach to Fraudulent Claims Generally: Fairclough Homes v Summers [2012] UKSC 26
Bill Perry and Ruby Modare