Cybersecurity and the Law Firm

by
Mr. Dmitri Hubbard,
General Counsel,
Blue Dragon Asia

Based in Hong Kong since 2002, Dmitri consults on a wide range of contentious legal problems which arise at the intersection of law and technology. Dmitri uses his experience in managing over 200 investigations since 2009 in Asia to preach about best practice and responding to crises.

His focus is on internal and regulatory investigations, international and Asian litigation, cyber security and data privacy compliance scenarios across Asia-Pacific. He works closely with large law firms and General Counsel for matters which have a Hong Kong or Asian dimension. Dmitri specializes in advising clients on regulatory and litigation matters involving data privacy concerns, forensic investigative needs, cyber breach, electronic discovery, data mapping, evidence management, document review and analysis.

Since in Asia, Dmitri has held Regional Management Roles at LexisNexis, Epiq Systems, Control Risks Group, Xerox, Conduent, and Blue Dragon Asia. He has been an adjunct lecturer / professional consultant at the three HK University Law schools (HK University, Chinese University & City University).

Dmitri is a qualified Barrister and Solicitor of the High Court of New Zealand. Dmitri holds a Bachelor of Laws, a Master of Laws (focusing on international commercial law) and a Bachelor of Arts in English Literature and Economics from Victoria University of Wellington. He holds a Diploma in International Trade and Shipping Law from London Guildhall University, and has done the HK SFC licencing exams for securities dealing, derivatives dealing, corporate finance and financial markets. He frequently presents at industry seminars, professional associations and regional conferences across Asia. He has written several books and articles on HK and Asian data privacy, cyber security, ediscovery, law of evidence, employment and contract law.

"If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology" **Bruce Schneier, Cryptographic Expert**

"For a lot of firms, they think the Panama Papers scenario won't happen to them..." **Data Privacy Officer, Major US Law Firm**

This seminar explores why and how law firms are exposed to cyber security risks and attacks which put their data, clients, and personnel at risk. It then goes on to make suggestions to minimize that risk and respond to threats and vulnerabilities.

An attendee will go away with a strong understanding of the attractiveness of a law firm as a target for a cyber actor, the biggest targets, threats and vulnerabilities.

An attendee will also gain practical insight as to how a law firm can combat these threats and vulnerabilities, from a variety of procedures, technologies and behaviours.

Law firms are at a serious turning point where they are putting in place expertise, systems and technology to counter the growing cyber risk that they face.

Across three hours, we hope to answer the following three questions, each taking approximately one hour:

1. Why law firms?

- Law firm as gatekeepers and agents
  1. Between client and vendors
  2. With vendors for own purposes
  3. Access to
     - Network
     - Email
     - Premises
- Legal Professional Privilege
  1. Privilege points to things of value
  2. Privilege is a legal obligation on the law firm
  3. Legal responsibility points toward needs for greater security
- Personal Data Treasure Trove
  1. Client personal data
  2. Privilege/confidentiality induces sharing
  3. Advanced warning on deals/litigation strategy/persons involved
- Companies trust with trade secrets
  1. Trade secrets
  2. Customer lists
  3. IP/IT and other confidential information
- Security weakest link
  1. Compared to scale/budgets of biggest clients
  2. Geographic spread/small offices
  3. IT/CIO/Risk officers spread thin
- Partnership structure
  1. Decentralised
  2. Independent work flow of partners
  3. Proliferation of devices, softwares, systems
- Traditional, Protected Businesses
  1. Focus is on practice of law
  2. Monopolistic protections
  3. Follow client to firm - pick targets
- High possibility of embarrassment
  1. Value of data
  2. Panama Papers
  3. Cyber insurance
- In-house Expertise
  1. Some partners are cyber experts
  2. Pick targets from more senior/less technical/younger, less aware
  3. An individual partner vs a community of hackers
- Risk management approach
  1. Not enough focus on cyber security at senior level
  2. Attendance of internal seminars - partners too busy
  3. Culture issues

2. How law firms?

- Insider threats
  1. Employee negligent revealing information
     - Passwords
     - Information/data
     - Install dangerous software
     - Old version OS
     - Unpatched device
  2. Employee fooled via social engineering
     - Click a link/phishing/spear phishing
     - Give someone a password/malicious actor
     - False wifi setup & man in the middle attack
  3. Employee not negligent by nevertheless does something to expose the network
  4. Employee deliberate leak
     - Disenfranchised employee
     - Going to a competitor
     - Starting own business
  5. One of the above 1-4, involving a third party contractor on premises
  6. One of the above 1-4, involving a vendor or partner
  7. One of the above 1-4, involving a client-side breach
- Patching vulnerability (software)
  1. Known patched problems
     - Patch not applied
  2. Unknown unpatched problems
- Device vulnerability (software or hardware)
- Malware - malicious software
  1. Definition
     - Trojans (70%)
     - Viruses (17%)
     - Worms (7.8%)
     - Adware (2.2%)
     - Backdoors (1.9%)
     - Spyware (0.08%)
  2. Examples
     - 2013 Toronto law firm lost hundreds of thousands in a Trojan attack replicating a bank website and copying the passwords and accounts as a bookkeeper typed them in. This gave hackers full access to the account.
- APTs (Advanced Persistent Threat)
  1. Definition
  2. Examples
- DDOS Distributed denial of service attack
  1. Definition - crowding the shop door
  2. Examples
- Phishing
  1. Definition
  2. Examples
- Spear Phishing
  1. Definition
  2. Examples
     - 2012 Virginia law firm victim to a spear phishing attack. Hackers infiltrated the email system, and released confidential information relating to high-profile cases.
- Ransomware
  1. Definition
  2. Examples
     - 2014 small US law firm falls victim to Cryptolocker - unable to retrieve files in time and didn't pay ransom. Theives made $30 million from Cryptolocker.
- Brute force/web page vulnerabilities/web form vulnerabilities
  1. Definition
  2. Examples

Scan to Calendar

The PROFECTIONAL Company®
Professional Services to the Perfection
Telephone: **+852 3118 2371** | Facsimile: **+852 3118 2372**
Email: **info@profectional.com** | Website: **http://www.profectional.com**
Address: **P.O. Box 9993, General Post Office, Hong Kong**

KORNERSTONE
Training. Makes a difference.
Telephone: **+852 2116 3328** | Facsimile: **+852 2116 3571**
Email: **enquiry@kornerstone.com** | Website: **http://www.kornerstone.com**
Address: **15/F, Hip Shing Hong Centre,**
55 Des Voeux Road Central, Central, Hong Kong

3. What can law firms do in response?

- Cyber response & intelligence
  1. Having a plan
     - Roles and responsibilities
     - Locations/communications
       - War room setup/planning
       - Email & IM
       - Phone/vidcon
     - Pre-prepared scenarios & types of incidents
       - Contained
       - Uncontained
       - Severity
     - Having an understanding of threats
       - Nation states
       - Cyber criminals
         - Deep web
         - Dark web
         - Threat intelligence
       - Cyber activists
         - Blurring of categories
- Access and Control
  1. Concepts around administrative access
     - Admin and activities
     - "Over privileged" users - principle of least privilege
  2. Use of Encryption
  3. Use of VPN
  4. Control of devices - BYOD/IoT
  5. Control of softwares used
- Training & more training
  1. Self-regulation
  2. Awareness of risks
  3. The modern workplace/time/medium
- Legacy Systems
  1. Old devices/operating systems
  2. Mapping with uncover
  3. Judge by the weakest
- Data mapping
  1. SANS criteria for security - figure how to defend
  2. Crown jewels/data audit - figure what is worth defending
  3. Problems with previous approaches
     - Security by obscurity
     - Protect everything is protecting nothing
     - Perimeter defences do not work
- Risk management
  1. Risk-based approach
  2. ISO/SANS
  3. Data privacy in the spotlight
- Chain of command
  1. Ownership at a senior level
  2. Harmonised approach across divisions
- Conversation with clients and vendors
  1. Partnerships require communication
  2. More understanding reduces risk
- Password management & patching
  1. Review password practices
  2. Review permissions (no broader than necessary)
  3. Review admin rights
  4. Review systems around leaving/incoming employees
- Post mortems
  1. Summarise problem from IT and legal perspective
     - Date/time of incident
     - Location/function of system/device
     - How identified problem
  2. Focus on what happened (not whose fault)
     - Steps to contain problem
     - Impact of the problem
     - Persons involved in solving problem
  3. Discuss how to prevent in future
     - Meeting notes/reports of post mortem must be kept secure
     - Monitor activities associated with breach closely
     - Deduce whether incident random or targeted
  4. Focus on lessons learned
     - Unpatched vulnerabilities?
     - Volume of genuine alerts/false alerts
     - Metrics and time to respond
  5. Focus on channels for response
     - Follow up actions
     - Education gaps
     - Technology/process gaps
  6. Refine cyber response plans

Code:	**EVT000000230**	Level:	**Advanced**
Date:	**30 July 2018 (Monday) - Cancelled**	Language:	**English**
Time:	**14:30 - 17:45** (Reception starts at 14:00)	Accreditation(s):	**LSHK RME Elective Course** **LSHK 3.0 CPD Points**
Venue:	**Kornerstone Institute** 15/F, Hip Shing Hong Centre 55 Des Voeux Road Central Central, Hong Kong	Request for Rerun:	**Please Contact Us for Details**

The PROFECTIONAL Company®
Professional Services to the Perfection
Telephone: **+852 3118 2371** | Facsimile: **+852 3118 2372**
Email: **info@profectional.com** | Website: **http://www.profectional.com**
Address: **P.O. Box 9993, General Post Office, Hong Kong**

KORNERSTONE
Training. Makes a difference.
Telephone: **+852 2116 3328** | Facsimile: **+852 2116 3571**
Email: **enquiry@kornerstone.com** | Website: **http://www.kornerstone.com**
Address: **15/F, Hip Shing Hong Centre,**
55 Des Voeux Road Central, Central, Hong Kong