Seminar on Unfair Competition Enforcement in the United States and Supply Chain CybersecurityIssues

Palace Hotel Saigon, HCMC, November 19th 2014
Seminar on Unfair Competition Enforcement in the United States; Supply Chain and Cybersecurity Issues

Palace Hotel Saigon, HCMC, November 19th 2014

MICHAEL MUDD
Secretary – General, Asia – Pacific & MEA
The Open Computing Alliance-London, UK.
Senior advisory board member, OSAC, Hong Kong
Today

- Business Risk
- Cyber Threats
- Risk Mitigation
- Best Practices for Data Protection
- Further Thoughts and Action
Planning for *all* probabilities -
- Damage to Business Relationships
- Caused by: Man Made; Natural; Business; *Legislative*

- Malware risk from *infected software*
- Legal risk from enhanced *trade and IP laws*
- Non action is a *reputational risk*
Unfair Competition laws in the US

- Laws that seek to prosecute *IP theft* in the supply chain.
- Only companies who do *not pay* for the IT used in their business processes are at risk.
- The risk of malware infections from copy software is high – up to 95% in some countries.
- The Attorney General or other parties may bring civil lawsuits in any US state.
- UCA Applies to *all* entities in the supply chain.
The Threat

Online commerce by definition means servers are connected via the public Internet

There is no longer E commerce, there is only commerce that is *Enabled* by IT

Cloud services are everywhere today running social media and the biggest online stores in the world

There are a lot of bad actors out there trying to steal from the 1+ billion users of the Internet...
Cyber attacks on the increase

- Web-based malware attacks *doubled in the second half of 2013.*
  - Web-based attacks represented 26% of total
  - Conficker worm next with 20%.
  - MAC attacks saw 51 new variants
- Mobile attacks on the increase.
  - Android accounted for 97% of all in 2013 and Symbian 3%
  - Nil on any other mobile O/S (BB/MSFT/IOS)
- Ouroboros Cyber weapon used in Ukraine 2014.
Most South Korean Credit Card Holders Have Details Stolen in Massive Breach
One Example - Target stores

- Date; Nov. 27 to Dec. 15 2013.
- Malware entry was via a supplier...
- Credit card data stolen ; 40 Million (sent to Russia).
- Estimate fraud per card ; $300*.
- Total value of fraud ;$1.4-2.2bn*.
- Losses to both banks and Target ($420m).
- Does not include fines for data breach and loss of reputation.
- It cost the CIO then the CEO/Chairman their jobs...

© Asia Policy Partners/Open Computing Alliance 2014

*Jeffries Securities 2014
What do Exporters really WANT?

- To deliver products and services with:
  - Data Security
  - Confidentiality
  - Integrity
  - Availability

- To comply with industry regulators.
- To comply with data privacy laws.
- To reduce costs and improve service.
- To respond to customers needs faster.
- To increase profits.
What do US Customers DEMAND?

- Suppliers to manage their own IT risk to minimise their exposure to malware threats.
- Suppliers may look at IT and data under the ‘3 P’s.’*
  - Principles
  - Preparedness
  - Partnerships
- This will enable a supplier to deliver services with:
  - Confidentiality
  - Integrity
  - Availability
- Satisfying both the UCA laws and managing data security risks for their own operations and that of their customers.

An IT/IP Risk Mitigation Framework

“*If you protect your paper clips and diamonds with equal vigor, you will soon have more paper clips and fewer diamonds*”

Dean Rusk  (US Secretary of State, 1961 – 1969)

- Start with simple data classification
- Know your risks. What are they, where are they?
- Behind every security problem is a human being
- Do have antivirus on *every* machine - Including mobile and tablets
- If you need help, consider Cloud Service Providers

Work with your customer closely; make it clear that you take care to protect them

Someone in your organisation must be ultimately responsible
The Safe Data Principles Framework*
Create a Cybersecurity Framework

- **Include** a set of standards, methodologies, procedures, and processes that align policy, business, and technological approaches to address cyber risks.

- **Provide** a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk.

- **Identify** areas for improvement that should be addressed through future collaboration with particular sectors and standards-developing organizations, enable technical innovation and account for organizational differences include guidance for measuring the performance of an entity in implementing a Cybersecurity Framework.

Courtesy Tim Grance, Cybersecurity Head, NIST 2014
Identifying and mitigating risk

- Enables organisations to establish a roadmap to reduce cybersecurity risk
- Can be used to describe current state and desired target state of specific cybersecurity activities
- Created by determining which Categories are relevant to a particular organisation, sector, or other entity
- An organisation’s risk management processes, legal / regulatory requirements, business / objectives, and organisational constraints

Courtesy Tim Grance, Cybersecurity Head, NIST USA 11/18/2014
If using an external SP, know where your Data will be located. (ISO 27018).

Data owners should ensure that government policies, economic and legal conditions of the identified data locations are safe and stable.

SPs should not use Data for any purpose other than that which is necessary to provide the Cloud Service. (ISO 27018).

The contract should prevent SPs from using Data for any secondary purpose at all times. (ISO 27018).

Customer Data must be segregated from other Data held by the SPs. SPs must be able to identify the Customer Data and at all times be able to distinguish it from other Data.

SPs should use encryption technology that meets or exceeds international standards to protect and secure the Data at all times. (ISO 27018 requires encryption of PII over public networks).
SPs may only use subcontractors if the subcontractors are subject to equivalent controls as the SP.  
Data Owners must carry out, and SPs must assist in facilitating, a risk assessment and due diligence on the SP to ensure that the SP and its services meet the legal, regulatory, contractual and business requirements. 
Data Owners should have in place a risk management plan that includes measures to address the risks associated with the use of external Data Centres or Cloud Services. 
SPs must provide regular reporting and information to demonstrate continued compliance with the legal, regulatory, contractual and business requirements throughout the duration of a contract. 
Data Owners and SPs must meet regularly to review the reports and performance levels.
A Framework – AVAILABILITY

- External services must be reliable and be able to document that reliability.
- SPs must have an effective business continuity plan with appropriate service availability, recovery and resumption objectives and with regularly tested and updated procedures and systems in place to meet those objectives.
- The risks of downtime should be minimized through good planning and a high degree of system resilience.
- Data owners must have appropriate exit provisions in the contract with the SP. To the extent that the Owner requires, on termination the SP must work with the Owner to return the Data to the Owner and then the SP must permanently delete copies of that Data from the SP’s systems.
- Any Data that does not need to be returned to the Owner must be permanently deleted by the SP. (ISO 27018).
Data Confidentiality - protecting information and respecting privacy

• Today it is **essential** that security and personal data privacy protection become a priority throughout all levels of the organization.

• Develop a security and privacy protection Framework based on Industry and ISO security standards, universal personal data protection principles and compliance with regulations and privacy laws.

• Have the Framework externally certified for adequacy, to build and maintain customers’ trust and confidence.

• Build and sustain a culture to protect information and respect privacy through education, technology, processes and procedures.

• Senior Management and Board of Directors’ commitment is critical, any failures will reflect directly on them. (see Target...)

© Asia Policy Partners/Open Computing Alliance 2014
ISO 27018 is a new international standard for the protection of personal data in the Cloud, based on the strong EU data protection laws.

Compliance with ISO 27018 can be assessed by a 3rd party during an ISO 27001 audit.

ISO 27018 reduces risk for your US customers and enhances confidence in your care and attention.

The OCA has prepared a White Paper outlining what ISO 27018 does and why it assists in Cloud adoption.
Data Confidentiality – Other Standards, Audits and Certifications

ISO
International Organization for Standardization
27001, 23001 & 31000

European Commission
Article 29 compliance

FedRAMP
Ensuring secure cloud computing for the Federal Government

FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) IMPLEMENTATION PROJECT
Protecting the Nation’s Critical Information Infrastructure
Our Vision
To promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act including:

© Asia Policy Partners/Open Computing Alliance 2014
The Cloud provides an extra layer of Data security

- Help protect on-premises, hybrid and cloud infrastructure with layered security
- Encrypt individual files, folders, and removable storage devices
- Create persistent, secured connections & enable multi-factor authentication
- Unify management with a single administrator console
- Proactively meet your compliance needs and ensure data privacy
in combination with protected devices

- Use devices with secured start-up and full-featured anti-malware
- Prevent unauthorized access to data and remotely wipe devices
- Provide single sign-on with support for virtual smartcards and biometrics
- Manage PCs, Windows devices, Apple iOS, and Android devices
- Configure policies with granularity to lock down functionality as needed
Most companies have got the physical supply chain risks well sorted out.

However the IT security, legal, regulatory and compliance issues of have not been addressed by the majority of companies with respect to their suppliers' IP practices.

Suppliers/manufacturers may install too much IT, so a software management audit may reduce costs and increase productivity.

Respecting UCA laws will benefit customers in the US by providing legal certainty from suppliers, enhancing trust in their suppliers products and processes – and driving an increase in business.
To prepare for this significant shift in trade risk, exporters to the US need to take action now:-

1. If software is used in compliance with most countries IP laws, it will usually comply with UC requirements
2. This will also harden your defences against malware
3. To verify licensing, conduct a software audit working with your IT supplier and demand your suppliers to do the same
4. There are automated tools available to assist in this
5. Responsible exporters will make this part of the regular export documentation for all customers in the US

An opportunity for firms to advise their US customers now to prevent a letter from the AG!
Service Providers/Data Owners and Exporters are recommended to consider adopting:

- **A Cybersecurity Framework *(February 2014)**
- **Safe Cloud Principles Framework (March 2014)**
- **ISO 27018 (July 2014)**

...To ensure they create a long lasting, safe and secure relationship with their customers in the US.
What next?

- Do consider Cloud computing which is facilitating the next level of commerce today.
- Do implement layered security from the edge (the weakest) to the centre (the ‘Fort Knox’ defence) which is enhanced in the Cloud.
- Do protect what is important, not what is just ‘data’.
- Don’t be like Targets supplier and be the ‘Trojan horse’ to your customers in the US (or anywhere).
- Do ask your Service Provider how Cloud can help you achieve this whilst working within all regulatory and best practice guidelines and laws.
Acknowledgments
NIST; Tim Grance, Cybersecurity Head
Microsoft; Pierre Noel, Chief Security Officer Asia

THANK YOU!
MICHAEL MUDD
+(852) 2830 9936

MMUDD@ASIAPOLICYPARTNERS.COM
WWW.OPENCOMPUTINGALLIANCE.ORG

11/18/2014
The OCA

- UK based global ICT industry policy think tank, plus advocacy.
  - Members include technology leaders in Asia-Pacific economies.
- Creating Dialogue on Technology and Trade Policy;
  - Open Innovation and Competition.
  - Open Standards.
  - *Fair trade and respect for Intellectual Property.*
  - *Cloud Computing for Secure & Trusted IT.*
  - Energy efficient IT processes.
- ...to drive positive outcomes for all stakeholders - both public and private.
- Office in Hong Kong for Asia Pacific*.
  - mmudd@opencomputingalliance.org
  - www.opencomputingalliance.org

* Represented by Asia Policy Partners LLC