Data Breaches and Trade Secrets: What to Do When Your Client Gets Hacked

- R. Mark Halligan, FisherBroyles, LLP
- Andreas Kaltsounis, Stroz Friedberg
- Amy L. Carlson, Stoel Rives LLP

  - Moderated by David A. Bateman, K&L Gates LLP

ABA Section of Intellectual Property Law

2015 ABA Annual Meeting

Discussion Outline

1. Trade Secret Fundamentals

   R. Mark Halligan, FisherBroyles, LLP

2. Who is Stealing Your Trade Secrets?

   Andreas Kaltsounis, Stroz Friedberg

3. Breach Planning and Response -- A Privacy Perspective

   Amy L. Carlson, Stoel Rives LLP

Trade Secrets and Data Breaches

R. Mark Halligan, Esq.

FisherBroyles, LLP

American Bar Association Annual Meeting 2015

The Modern Definition of a Trade Secret

Restatement Third Unfair Competition:

"A trade secret is any information that can be used in the operation of a business or other enterprise and that is sufficiently valuable and secret to afford an actual or potential economic advantage over others." [Section 39]

What is a Data Breach?

A data breach is an incident in which sensitive, protected or confidential *data* has potentially been viewed, stolen or used by an individual unauthorized to do so. Data breaches may involve personal health information (PHI), personally identifiable information (PII), *trade secrets* or intellectual property.

What is a Trade Secret?

The Illinois Trade Secrets Act:

"Trade secret" means information, including but not limited to, *technical or non-technical data*, a formula, pattern, compilation program, device, method, technique, drawing, process, financial data, or list of actual or potential customers or suppliers…….

Two sides of the Same Coin

DATA……BREACH

TRADE SECRET……MISAPPROPRIATION

No Value Without Identification

Appropriate security relies on identification

+

Failure to properly secure trade secrets results in forfeiture of rights

=

Unidentified and unprotected trade secrets result in a zero economic valuation

Two Ships Passing in the Night

Non-public personal information

Non-public proprietary and confidential information

Lot's of attention to privacy and data breaches

Very little attention to the management of trade secret information

Identification – What Gives?

- Despite the known value of trade secrets, many issues work against identification projects
  - Large number of trade secrets even in small companies
  - Reliance on time-intensive manual methods

  Lack of methods that span the range of trade secrets
- What is needed are solutions to these issues
  - Methods must reduce the scope of the problem
  - Automated methods must emerge
  - Methods must apply across all types of trade secrets

Identification – Current Status

Most companies do not have any structured system in place to identify, value, and protect trade secrets

- Systems that do exist are ad hoc or interim
- The “state of the art” in trade secret protection right now is – “we are working on it”

Trade Secret Audit - Method

- Interviews
- Categorization/Prioritization
  - Collecting SFP information during interviews makes this step easy
- Classification into confidential, secret, etc.
  - Classification can be made easier by being the same for all trade secrets in the same SFP

Trade Secret Audit - Methods

- Manual audits by internal staff ????
- Manual audit by outside consultants
  - Faster
  - Well-practiced methods
  - Know company, its employees, and its business
  - Slower, but likely more thorough
- Computer-automated audits
  - Technological Advances—Merger With Data Privacy
  - Combines advantages of internal and external audits

Valuation – The Six Factors

The First Restatement of Torts provides six factors for courts to consider in determining existence of a trade secret:

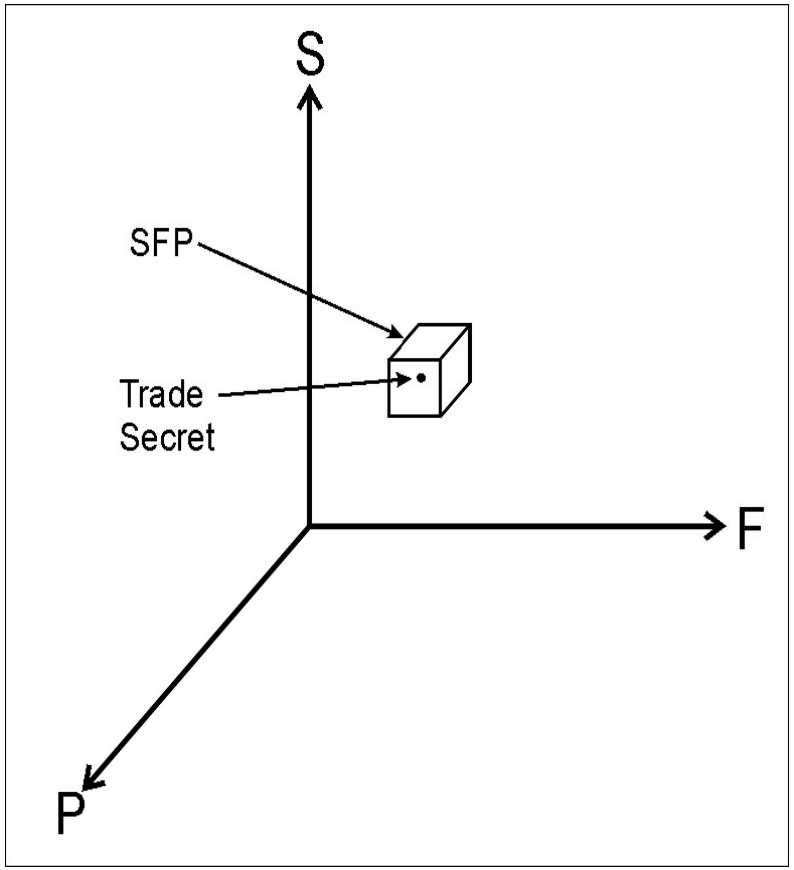
1. How widely is the trade secret known within the company?
2. How widely is the trade secret known within the industry?
3. How much time, effort and moneyhas been invested to develop this trade secret?
4. What is the economic benefit of the trade secret?
5. How hard would it be to independently reproduce the trade secret?
6. What security measures have been taken to protect the trade secret?

Applying The Six Factors

- The greater the compliance with the six factors, the more likely a court will find that the information qualifies for trade secret protection
- In practice, the most valuable trade secrets in the company have high compliance with the six factors

Defining the Space

- The SFPs form a three-dimensional space within which all the company's trade secrets can be mapped
- Each trade secret lies within one SFP



SFPs

- An SFP is a trade secret category:
  [Subject] [Format] for [Product]
  - **Subject:** the department or functional area within the company or division
  - **Format:** the form of the trade secret itself, such as a method, design, plan, forecast
  - **Product:** the product or family of products to which the trade secret applies

SFPs - Examples

- Manufacturing Process for Transmissions
  - Subject Format Product
- Research Test Results for Non-Flammable Plastics
  - Subject Format Product
- Advertising Roll-out Strategy for New Cola
  - Subject Format Product
- Software Source Code for Operating System
  - Subject Format Product

SFPs – Ease of Implementation

- For a company with 10 major functional areas, 30 trade secret formats, and 20 separate product areas, 6,000 SFPs are automatically defined
  - Some SFPs will be empty. There will be no "Sales Test Results" for example.
- SFPs require no employee training

SFPs - Benefits

- Before any specific trade secrets are identified, they can be classified and prioritized
  - Trade secrets in the same SFP are likely to share the same level of sensitivity
  - The most valuable trade secrets will cluster within identifiable SFPs
  - SFPs allow “triage”, the prioritization of efforts on the SFPs with the most sensitivity and the highest economic value

Trade Secrets and Data Breaches

Andreas Kaltsounis, Vice President
STROZ FRIEDBERG

American Bar Association Annual Meeting 2015

Who is stealing your IP?

Insiders

REUTERS

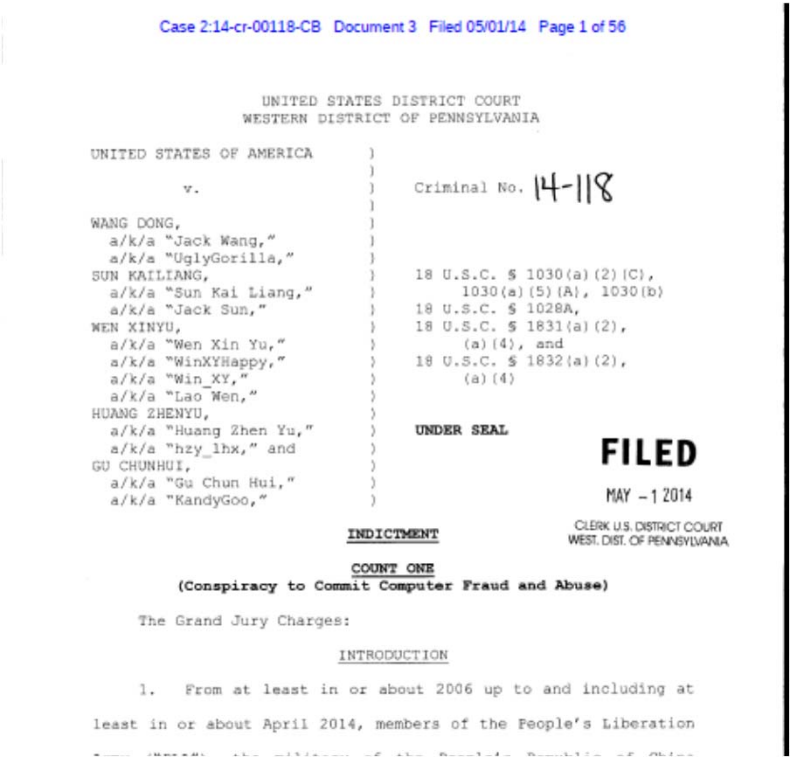
Ex-Goldman programmer indicted over HFT code theft

NEW YORK (Reuters) - A former Goldman Sachs Group programer was indicted on charges he stole computer code for the investment bank's high-frequency trading platform, federal prosecutors said on Thursday.

The former programer, Sergey Aleynikov, 40, was arrested and charged in July. The three-count indictment alleges that Aleynikov, who worked at Goldman from May 2007 to June 2009, illegally transferred and downloaded "hundreds of thousands of lines of source code for Goldman's high-frequency trading system" on his last day at the firm.

Aleynikov, according to the indictment, then uploaded the source code onto a laptop computer that he took with him to a meeting in Chicago with his new employer, Teza Technologies LLC, a high-frequency trading

Cyber-Espionage Actors



Case 2:14-cr-00118-CB Document 3 Filed 05/01/14 Page 1 of 56

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF PENNSYLVANIA

UNITED STATES OF AMERICA)
)
v.) Criminal No. 14-118
)
WANG DONG,)
a/k/a "Jack Wang,")
a/k/a "UglyGorilla,")
SUN KAILIANG,) 18 U.S.C. § 1030(a)(2)(C),
a/k/a "Sun Kai Liang,") 1030(a)(5)(A), 1030(b)
a/k/a "Jack Sun,") 18 U.S.C. § 1028A,
WEN XINYU,) 18 U.S.C. § 1831(a)(2),
a/k/a "Wen Xin Yu,") (a)(4), and
a/k/a "WinXYHappy,") 18 U.S.C. § 1832(a)(2),
a/k/a "Win_XY,") (a)(4)
a/k/a "Lao Wen,")
HUANG ZHENYU,)
a/k/a "Huang Zhen Yu,") UNDER SEAL
a/k/a "hzy_lhx," and)
GU CHUNHUI,)
a/k/a "Gu Chun Hui,")
a/k/a "KandyGoo,")

FILED
MAY – 1 2014
CLERK U.S. DISTRICT COURT
WEST. DIST. OF PENNSYLVANIA

INDICTMENT

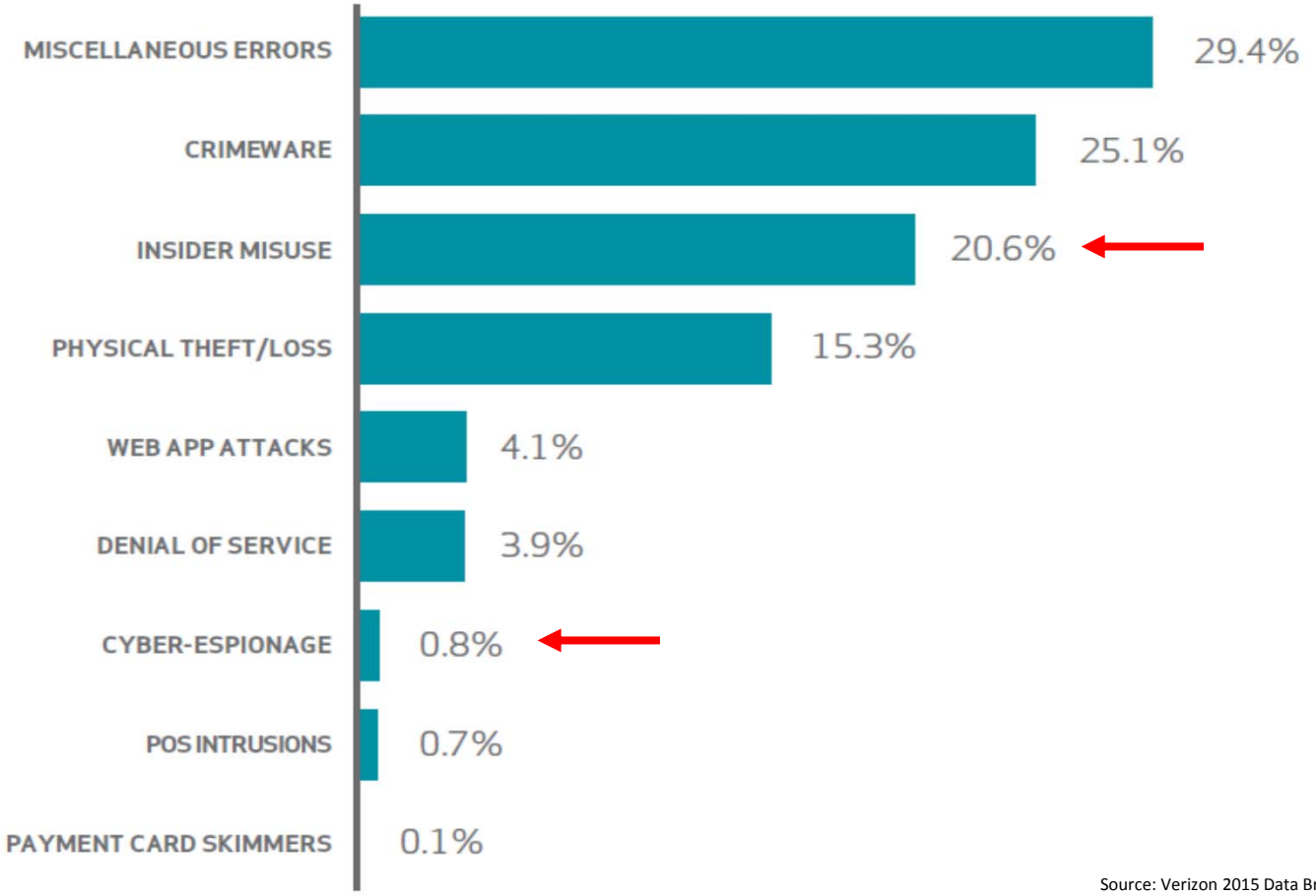
COUNT ONE
(Conspiracy to Commit Computer Fraud and Abuse)

The Grand Jury Charges:

INTRODUCTION

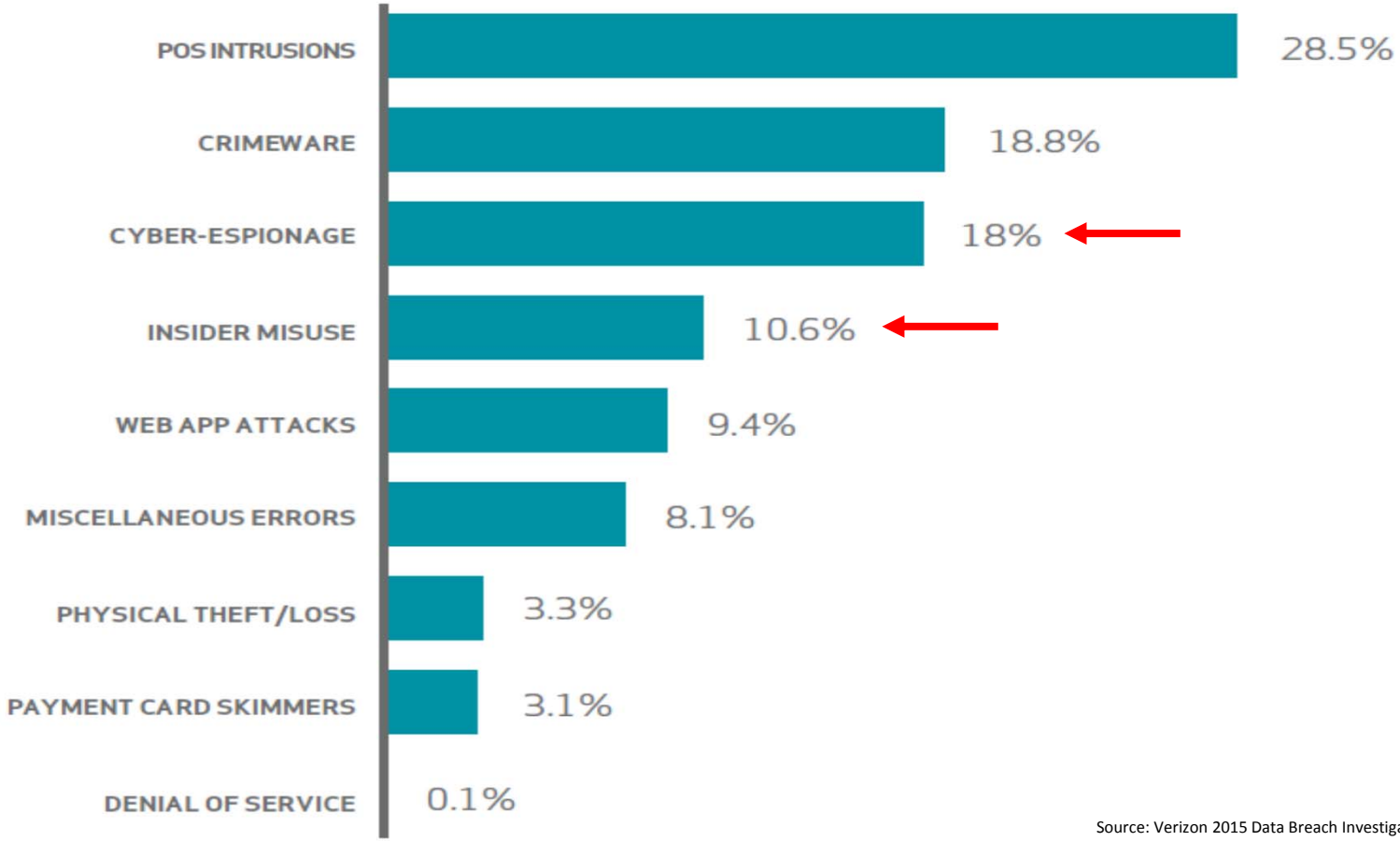
1. From at least in or about 2006 up to and including at least in or about April 2014, members of the People's Liberation

Quantifying the Problem – Security Incidents



Source: Verizon 2015 Data Breach Investigations Report

Quantifying the Problem – Confirmed Data Breaches



Source: Verizon 2015 Data Breach Investigations Report

Quantifying the Problem – Espionage Incidents vs. Breaches

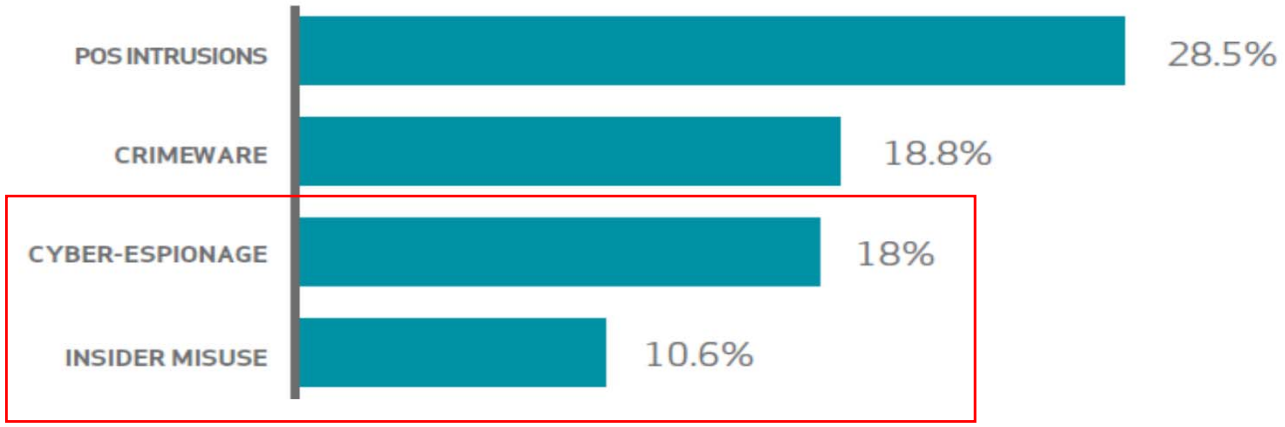
Cyber Espionage is:

- 0.8% of all security incidents
- But 18% of data breaches

Espionage lost in the avalanche of security incidents

Espionage is **targeted** and **persistent**

Quantifying the Problem – IP Theft is a Substantial Problem



Espionage + Insider Misuse = 28.6% of all breaches

How are they stealing your IP?

Insiders

- Where is the data?
- How is it stolen?

Espionage Actors

- APT Attack Lifecycle
- Main attack vectors
  - Malicious Emails
  - Watering-hole Attacks

Insider Theft Chess Pieces

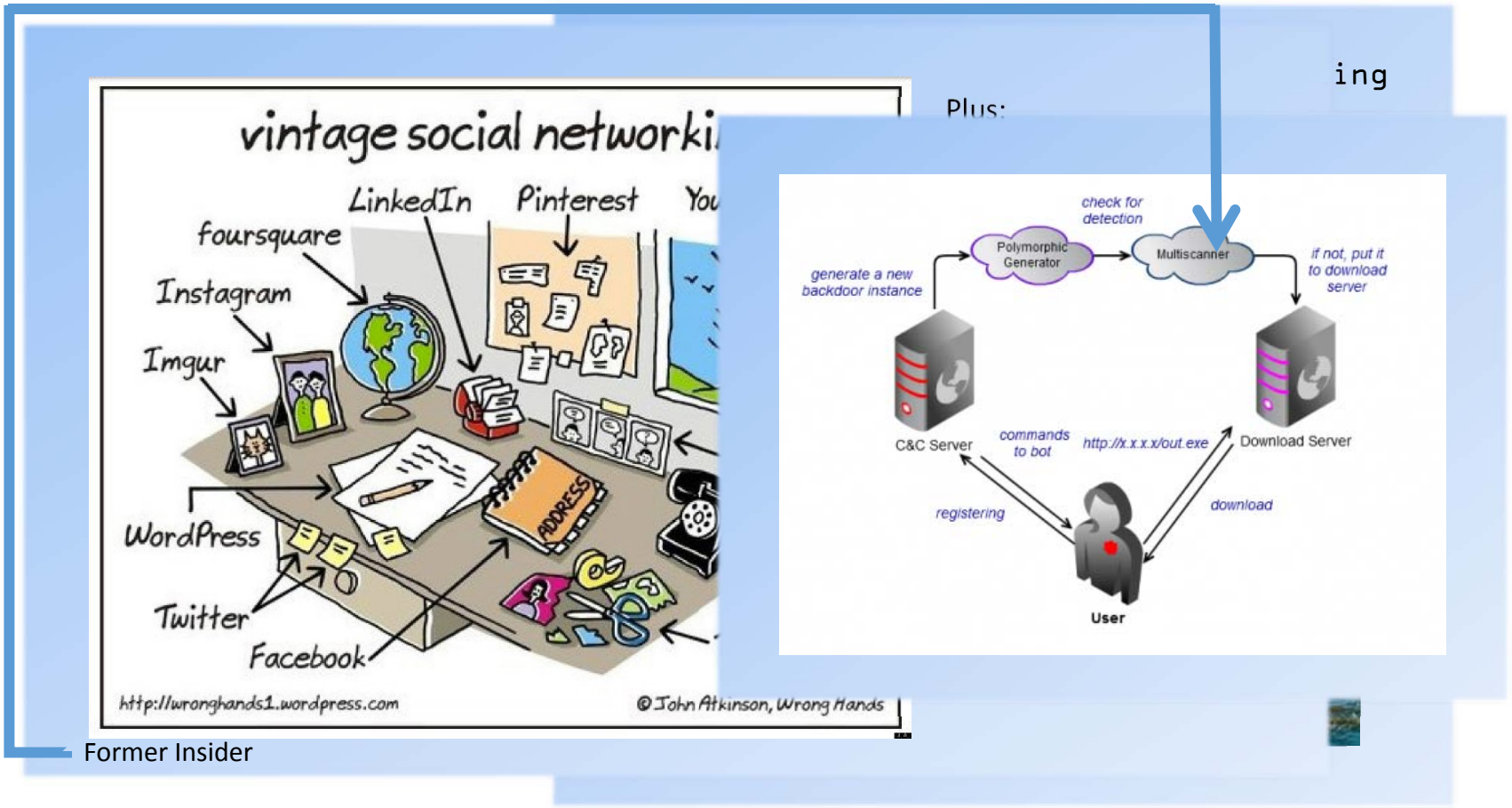

EMAIL SERVER


FILE SERVER

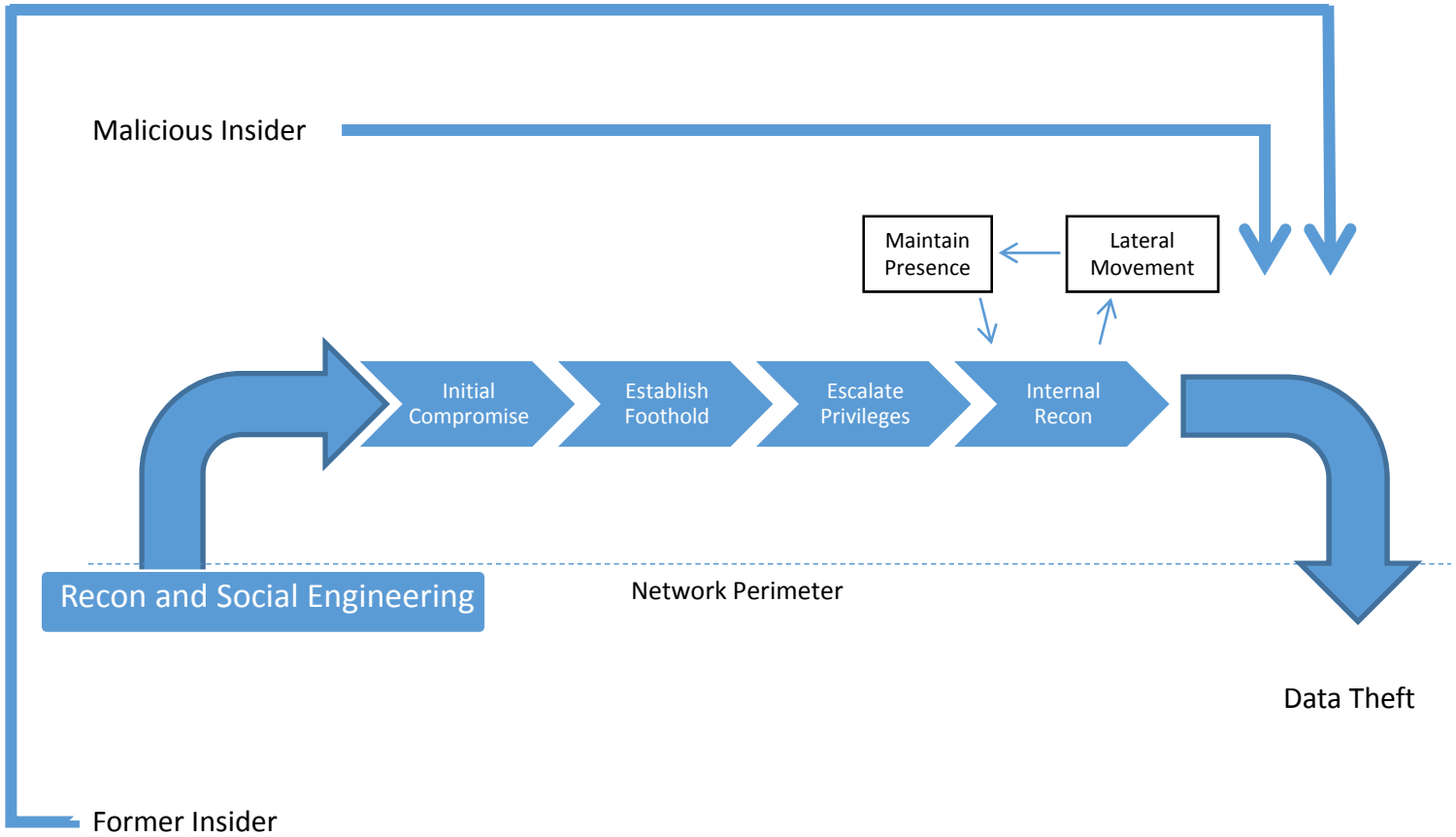

EXTERNAL MEDIA


LAPTOPS AND DESKTOPS

APT Attack Lifecycle



APT Attack Lifecycle



TRADE SECRETS AND DATA BREACHES – A PRIVACY PERSPECTIVE

Amy L. Carlson
Stoel Rives LLP

American Bar Association Annual Meeting 2015

COMPANIES ARE NOT PREPARED FOR DATA BREACHES

- Many companies wait until they experience a data breach to "prepare" for the breach
- Companies will often not know what data could be affected by an incident
  - No knowledge of all of the data on machines, networks or systems
  - No backups of lost, stolen or altered data
  - No logs that indicate which data was accessed
- When experiencing their first significant breach, companies generally have not entered into relationships with vendors to support incident response

OBVIOUS NEGATIVE RESULTS

- Delayed incident response
- Increased costs
- Regulatory fines
- Litigation
- Shareholder derivative lawsuits
- Loss of business
- Reputational harm

WITHOUT PREPARATION

- Each incident handled by those for whom it is a case of first impression
- Likely will not respond successfully to large incidents – time is the enemy
- No common benchmarking or reporting
- No understanding of causes of data breaches or focus on reducing data breaches
- No competitive advantage
- No insurance
- Will pay even if incident is caused by a vendor
- Customers will be very concerned if the incident is not handled professionally

WITH PREPARATION

- Prepared for a data breach
- Consistent, coordinated response
- Relationships with vendors are in place to respond to incidents
- Capable of handling a large incident
- Benchmarking and reports to understand data incidents
- Mature program will drive down the number of data breaches
- Competitive advantage
- Insurance will be available
- Contracts will address liability for data breaches
- Customers will observe a company that is prepared

MATURITY LEVEL – ARE YOU READY?

- Do employees know how to report incidents?
- Do vendors, subcontractors, temporary workers and others working in support of the company have an obligation to inform the company? Do they know how to reach the company?
- If there is a potential incident, will a knowledgeable person get the message and be able to help in a reasonable time frame?
- Who is on the Incident Response Team? Can you reach them on July 4th?

MATURITY LEVEL – ARE YOU READY?

- Do you have the resources to stop the incident or keep it from causing harm?
- Who is responsible for reviewing the incident?
  - Interviews
  - Forensic reviews
  - Physical investigation
  - Interaction with law enforcement
- Do you know how to preserve evidence?

MATURITY LEVEL – ARE YOU READY?

- Will you have any evidence to help you narrow down the impact of the incident?
- Will you have any policies, procedures, records of training and other privacy and safeguards documentation to demonstrate that the company addressed privacy and security of personally identifiable information prior to the breach?
- Do you have negotiated and signed contracts with vendors who will provide support during the incident? How do you reach them when it is an emergency?

MATURITY LEVEL – ARE YOU READY?

- Do you have a plan to respond to small and large incidents?
  - Can you stop the incident?
  - How do you plan to conduct an investigation of the incident?
  - Who will perform the forensic review?
  - Can you identify the individuals affected by the incident? Do you have their addresses?
  - Are you ready to prepare and send notification letters? Will you send letters if your customer's data is affected? Who is your mailing vendor?
  - Do you know if you need to inform a regulator? Will you inform a regulator for your customers?

MATURITY LEVEL – ARE YOU READY?

- Do you have a plan to respond to small and large incidents (cont.)?
  - What do you need to tell your customers? If the incident involves data owned by others, how do you plan to keep the data owners informed of the investigation and the steps taken to address the incident?
  - Are you able to set up a call center? Who will provide the support for the call center, and who will handle communications made directly to the company?
  - Who will provide you with legal counsel?
  - Who will prepare the incident website?
  - Who will provide public relations or crisis management support?
  - Who will provide services for affected individuals such as credit monitoring and credit restoration services?

MATURITY LEVEL – ARE YOU READY?

- Have you identified what can be handled internally and where you require support?
- Can you document your incident response?
- Have you tested your plan for responding?
- Have you negotiated who will handle the response and who will pay if the incident is caused by a vendor?
- Do you have insurance?
  - What does it cover?
  - Do you need to work with certain vendors to obtain maximum insurance coverage?
  - Are there any requirements (such as notification) for the company to use the insurance?

VENDOR REVIEW

- Review all vendors, including all vendors providing support for an incident.
- Create a Privacy and Security Intake Form for managing corporate projects and programs
- Create a Privacy and Security Questionnaire for potential vendors to use during the RFP stage
- Create standard privacy and security terms and conditions for procurement

VENDOR REVIEW

- Consider including privacy and security language in ALL contracts, even if you do not anticipate the vendor using personally identifiable information to perform under the contract
  - Would you have anticipated being compromised through your HVAC vendor?
- Obtain copies of vendor's privacy & security policies and procedures
- Obtain copies of any security reviews
- Obtain copies of self-audits or third party audits of compliance

COMMON MISTAKES IN REVIEWING CONTRACTS LANGUAGE

- Often asked to evaluate the "privacy clause" and nothing else
- Often asked to "just give me some privacy language"
- Many think only security clauses are necessary – and not privacy clauses
- Often brought in at the last minute
- Agreement/SOW/NDAs may already be signed by the parties!

KEEP PRIVACY T'S & C'S SEPARATE

- Negotiate privacy terms and conditions separately from traditional confidentiality clauses or other intellectual property terms and conditions
  - Often the carve outs from what is considered confidential do not apply to privacy protected data
  - Parties are often more willing to sign up to more stringent terms and conditions for privacy protected information
- Negotiations are easier if privacy is treated separately
  - The privacy and safeguards requirements often will not apply to other confidential information
  - Vendors will not agree to apply the more stringent requirements if it is not required or even best practices

PRELIMINARY STEPS FOR VENDOR CONTRACTS

- Identify types of data involved
- Diagram data flows, who will be doing what, with what specific data, at each stage of the data flow
- What parties are involved with the data?
- What laws apply to data?
- Where will data be accessed, used, processed?
- Will there be any access to company systems or just data?
- Will there be remote access?
- Even if the parties do not anticipate that data will be needed to perform under the contract, will the vendor have the potential to access data?

ISSUES WITH VENDOR CONTRACTS

- Often NO privacy clauses, or clauses very favorable to vendor
- Vendor generally will not pay in the event of a data breach unless liability is negotiated
- Often use confidentiality clauses that are not privacy specific, which may be contradictory to privacy requirements
- Often state that they will only comply with laws and regulations that are "applicable to the vendor"
- Often state that they will not be doing anything with the data, and clauses are not necessary (e.g., tier III support, collocation services, network design)

POLICIES

- Vendor must have, keep and update privacy and security policies and procedures
- Any changes must be more stringent, or obtain consent
- Provide copies or access to such policies and procedures
- Vendor must train on policies and procedures
- Consider having a standard training module for vendors providing support at the company or on company provided networks, systems and equipment

HOW TO DEFINE PRIVACY DATA

- Often there is NO definition in the contract
- Specific statutory definition (e.g., PHI, NPPI, Personal Data, Sensitive Personal Data, etc.)
- Use of the term personally identifiable information – what if it is sensitive, but not necessarily identifiable?
- Is data really de-identified? What is the de-identification standard?
- Data collected under a promise is privacy protected information
- Nonpublic information protected under privacy laws, rules and regulations or pursuant to contract
- In some circumstances, anything identifiable to an individual, regardless of its sensitivity

LIMITATIONS ON USES & DISCLOSURES

- What can the vendor, its affiliates and subcontractors do with the data? Remote access? Share de-identified data?
- Limit sharing within the company to those who need to know? Other limits on access?
- Training and signed NDAs for all who have the potential to use, access, transmit, or otherwise interact with data?
- Requirements specified by statute (e.g., HIPAA)?

LIMITATIONS ON USES & DISCLOSURES (CONT.)

- When would a vendor provide information to others, including individuals?
- Keep from using for another purpose
- Require disposal as soon as possible
- Decide who will provide access to data and how that will work between the parties when individuals have a right to request such information

SECURITY

- Security review – review answers to questionnaire or a prepared summary
- Create, maintain and enforce commercially reasonable policies, procedures and safeguards:
  - Confidentiality, integrity, availability and safeguarding of personally identifiable information
  - Protecting against reasonably anticipated threats, vulnerabilities, hazards and accidents to the security or integrity of personally identifiable information
  - Protecting against unauthorized sharing of personally identifiable information
  - Providing for disaster recovery
  - Updating he policies and procedures as required to address laws, regulations, and new threats, vulnerabilities, hazards and accidents
  - Benchmarking

SECURITY (CONT.)

- Which standards should the vendor comply with under the contract?
- Can the vendor self-assess or should is a third party assessment of compliance required?
- Draft terms and conditions to require vendors to address the most common ways data breaches occur for the company
- Draft terms and conditions to remediate security issues:
  - Encrypt unencrypted backup tapes
  - Limit locations for processing to certain countries
  - Comply with a standard (may need significant time to come into compliance)
  - Eliminate shared administrative passwords
  - Change hardware or software that is at end of life
  - Turn on adequate logging capabilities
- Ability to audit compliance
- Ability to have third parties perform reviews and conduct investigations

DISPOSAL

- What standard does the vendor have to meet?
- What disposal method for electronic and non-electronic information is acceptable?
- Is there a chain of custody?
- Is there an auditing protocol?
- Is there recordkeeping?

DATA BREACH

- Know if there are any specific laws or regulations or contractual terms which must be flowed down to the vendors providing support.
- If a Business Associate Agreement for Protected Health Information is flowed down, are additional privacy and safeguard terms and conditions required for personally identifiable information?
  - What constitutes a breach that is reportable to the company?
  - Some companies want to know about every security incident. Do you really want to know about every security incident even if the company's privacy protected data is not involved?

DATA BREACH

- What are the obligations of a vendor if there is a data breach?
  - Who makes the decision to give notice?
  - What if the vendor wants to give notice and the company does not think it is required?
  - What if the company wants to give notice, but the vendor does not think it is required?
  - Will vendor or company send the notice?
  - Which company will set up the call center?
  - Which company will provide for services for the individuals affected by the incident?
- Will the vendor indemnify company for a data breach? Internal and external costs?
- What insurance will the vendor be required to carry?