ISSA – Central Maryland Chapter

Risk Mitigation Strategies for Cybersecurity Service Providers

December 17, 2019

Razvan E. Miutescu

No professional courtesies…

Imperva Data Breach Caused by Stolen AWS API Key ...
https://www.trendmicro.com › vinfo › news › cybercrime-and-digital-threats
Oct 15, 2019 - **Imperva** recently revealed the primary cause of a **breach** that accidentally exposed customer **data** (which included email addresses, hashed ...

How Chinese Spies Got the N.S.A.'s Hacking Tools, and Used Them ...
https://www.nytimes.com/2019/05/06/us/politics/china-hacking-cyber.html
May 6, 2019 - ... **hacking** tools and repurposed them in 2016 to attack American allies and private companies in Europe and Asia, a leading **cybersecurity firm** ...

Customer data stolen as S.F. cybersecurity firm hacked, Stanford ...
www.siliconbeat.com/.../customer-data-stolen-s-f-cybersecurity-firm-hacked-stanford-...
Jun 1, 2017 - Stanford Medical School is reportedly a client of a **hacked cybersecurity firm** and used its services in connection with clinical trials.

Hacked government contractor shares breach details as ...
https://www.cyberscoop.com › miracle-systems-data-breach-sandesh-sharda
Sep 16, 2019 - CyberScoop could not independently confirm that only obsolete data from **Miracle Systems** was exposed in the **breach**. The Secret Service is ...

FireEye researcher hacked; firm says no evidence its systems hit
https://www.reuters.com/...cyber.../fireeye-researcher-hacked-firm-says-no-evidence-i...
Jul 31, 2017 - **Cyber security firm** FireEye (FEYE.O) said on Monday one of its researchers based in Israel had several of his online accounts **hacked** by ...

The Silent War: when cyber security companies get hacked - ET Tech
tech.economictimes.indiatimes.com › Latest Technology News › Technology
Jul 29, 2017 - **Cyber security firms** getting attacked by rivals in the business is quite common.

WTP Whiteford|Taylor|Preston LLP

Trustwave's lawsuits

- *Affinity Gaming v. Trustwave Holdings, Inc.*, U.S. District Court for the District of Nevada, Case No. 2:15-cv-02464:

  "Trustwave has engaged in similar conduct with prior clients – apparently, Trustwave's *modus operandi* is to conduct quick-hit investigations with minimal expenditure of effort, where it is paid a tidy fee for what ultimately ends up being essentially worthless services."

- *Trustmark Nat'l Bank, et al. v. Target Co. et al.*, U.S. District Court for the Northern District of Illinois, Case No. 1:14-cv-02069

  - Trustwave added as co-defendant re: Target's PCI compliance failure
  - Banks voluntarily dismissed lawsuit without prejudice to re-file

Other sources of legal risks

IP infringement litigation:

- *Strikeforce Technologies, Inc. v. Trustwave Holdings, Inc.*, U.S. District Court for the District of New Jersey, Case No. 2:16-cv-03573
- *Protegrity Corp. v. Trustwave Holdings, Inc.*, U.S. District Court for the District of Connecticut, Case No. 3:13-cv-1409
- *Symantec Corporation v. Zscaler, Inc.*, U.S. District Court for the District of California, Case No. 3:17-cv-04426

Regulatory enforcement:

- FTC settlement with Henry Schein Practice Solutions -- failure to provide the data security levels promised to customers ($250,000)
- HHS settlement with eClinicalWorks for selling faulty electronic medical records software and paying kickbacks ($155,000,000)

Open source and other “third party” materials
Data security flow-downs
“Compliance with all laws”
Warranties and Disclaimers
“Industry standards”
Limitations of Liability
Indemnification
Authorized Access
Illegal content (including child pornography)
“Hidden” expenses (litigation support), law enforcement, cooperation, data storage and disposal, etc.
Backup risks
Insurance
“MORE” …

Getting “inside” the client’s systems

Backup?

- Default – the customer’s responsibility
- Include backup obligations in Scope of Work

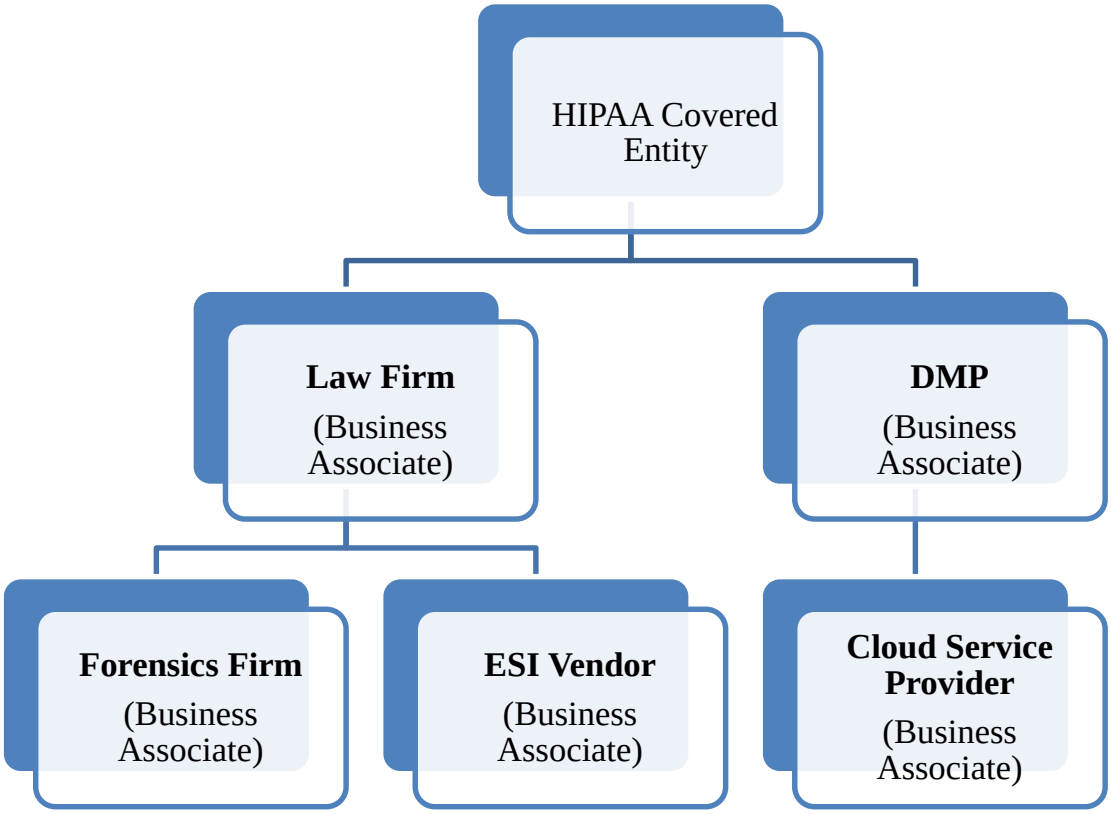
Authorized access

- Obtain written and detailed authorization from customer
  - Stored Communications Act
  - Computer Fraud and Abuse Act

Illegal Content

e.g., “child pornography shall be reported to law enforcement”

“Flow-downs”



"Compliance with all laws"

Compliance with Laws. The Company shall comply in all material respects with all laws, rules, regulations, orders and decrees of all governmental authorities . . .

… applicable to the operations of its business …

[… applicable to its obligations under this Agreement ….]

… *provided*, *however*, as a limitation on the foregoing general obligations, in the event any of Customer's Data is subject to any specific privacy, data security, or consumer protection laws, rules, regulations, orders or decrees, Customer shall so inform the Company prior to the execution of this Agreement.

Warranties and Disclaimers

As to information and computer programs provided under this Agreement . . .

. . . and except for the express warranties set forth in Section X (Warranties) of this Agreement . . .

. . . THERE ARE NO WARRANTIES (1) AGAINST INFRINGEMENT, (2) AGAINST INTERFERENCE WITH ENJOYMENT OF INFORMATION, (3) THAT INFORMATION, COMPUTER PROGRAMS, OUR EFFORTS, OR THE SYSTEM, AS EACH MAY BE PROVIDED UNDER THIS AGREEMENT, WILL FULFILL CUSTOMER'S PARTICULAR PURPOSE OR NEEDS, AND (4) AS TO DEFECTS IN THE INFORMATION OR COMPUTER PROGRAM WHICH AN EXAMINATION SHOULD HAVE REASONABLY REVEALED.

THE IMPLIED WARRANTIES OF MERCHANTIBILITY, FITNESS FOR A PARTICULAR PURPOSE, QUALITY, AND ACCURACY ARE HEREBY DISCLAIMED. THE INFORMATION AND COMPUTER PROGRAMS ARE PROVIDED "AS IS" AND "WITH ALL FAULTS" AND THE ENTIRE RISK AS TO SATISFACTORY QUALITY, PERFORMANCE, ACCURACY AND EFFORT IS WITH THE CUSTOMER.

Warranties as Marketing Tools

SentinelOne does not advise ransomware victims on whether or not to pay the ransom, but understands that there are times when it is necessary to recover data quickly. In the event that your organization must pay the ransom, SentinelOne Endpoint Protection Platform (EPP) customers covered by the SentinelOne Ransomware Warranty will be reimbursed up to $1,000 USD per affected endpoint if we're unable to keep you safe from a ransomware attack, and up to a maximum of $1,000,000 USD per company.

https://go.sentinelone.com

Our $100,000 cyber warranty, backed by AIG, helps pay for recovery expenses in the event you're breached under our watch. This ensures you're able to recover faster from a data breach and get back to business, which is critical when managing the fallout of a breach.

https://www.armor.com/cyber-warranty/

AsTech stands behind its work with a simple guarantee: if your company is breached through a source code vulnerability we miss, we'll pay up to $5M in breach related costs.

https://www.astechconsulting.com/astech-guarantee

"Industry standards"

The Company shall maintain appropriate systems security for its services in accordance with commercially reasonable industry standards and practices . . .

… to protect all of Customer's data and information from unauthorized disclosure or access …

… such systems security to include, among other things:

- minimum standards (e.g. access controls, transmission/storage security, encryption in transit and at rest, data segregation, personnel background checks)?
- IT management standards (e.g., ISO/IEC 27001:2005 – Information Security Management Systems – Requirements, ISO-IEC 27002:2005 – Code of Practice for International Security Management)?
- PCI DSS?

Limitations of Liability

Limitation of Liability. IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER OR ANY OF ITS AFFILIATES FOR ANY CONSEQUENTIAL, INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE OR EXEMPLARY DAMAGES (INCLUDING LOST PROFITS, BUSINESS OR GOODWILL) SUFFERED OR INCURRED BY SUCH OTHER PARTY OR ITS AFFILIATES, WHETHER BASED UPON A CLAIM OR ACTION OF CONTRACT, WARRANTY, NEGLIGENCE, STRICT LIABILITY OR OTHER TORT, OR OTHERWISE, ARISING OUT OF THIS AGREEMENT.

THE FOREGOING SENTENCE SHALL NOT LIMIT THE OBLIGATIONS OF EITHER PARTY TO INDEMNIFY THE OTHER PARTY FROM AND AGAINST THIRD PARTY CLAIMS UNDER THIS ARTICLE …

… AND SHALL NOT APPLY TO EITHER PARTY'S CONDUCT THAT IS GROSSLY NEGLIGENT, WILLFUL, FRAUDULENT, ILLEGAL, OR IN VIOLATION OF THAT PARTY'S OBLIGATIONS OF CONFIDENTIALITY OR DATA SECURITY UNDER THIS AGREEMENT.

Indemnification

The Company shall ***defend*** the Customer from and against all suits, claims, actions, demands, complaints, lawsuits or other proceedings, (collectively, "Claims"), that are ***brought by a third party***, …

… and shall ***indemnify*** and ***hold harmless*** to the fullest extent permitted by law the Customer from and against any and all losses, that arise out of or are attributable to a Claim of a third party, in connection with …

… (a) the Company's infringement of a third party's intellectual property rights, or (b) the Company's grossly negligent or willful misconduct in performing its obligations under this Agreement . . .

… provided, however, that the Company shall not be obligated to indemnify the Customer to the extent it is shown by evidence acceptable in a court of law having jurisdiction over the subject matter and meeting the appropriate degree of proof for such Claim that the Claim arose out of negligence or wrongdoing on the part of the Customer.

!!! OBTAIN BROAD INDEMNIFICATION FROM CUSTOMER !!!

“Open source” + “Third party materials”

“Open source” has the same meaning as the term “open source” promulgated and defined by the Open Source Initiative, available online at http://www.opensource.org/osd.html, as amended from time to time.

“**Third Party Materials**” means any proprietary software, open source code, data, ideas, concepts, know-how, tools, models, processes, methodologies, techniques, and other materials that were either originated by, developed by, purchased by, or licensed to a third party and which are licensed by Vendor from such third party.

“**Product**” means the software and technology, including any open source code and other Third Party Materials, and all related documentation, listed in the Specifications.

[…] warrants and represents that the Product, including any open source code and other Third Party Materials, does not violate, infringe, or misappropriate any intellectual property right of any third party.

Hidden expenses

Litigation support

- discovery
- subpoenas

Law enforcement cooperation

- reporting
- access to information

Data storage/disposal

- storage and disposal expenses
- specific legal requirements?

Insurance

Professional Liability (Errors and Omissions Liability), including Network Security and Privacy Liability with minimum limits of Five Million Dollars ($5,000,000) per claim and Ten Million Dollars ($10,000,000) in the aggregate.

The insurance shall include, at a minimum, coverage for risks associated with liability arising out of:

(1) Theft or unauthorized access or disclosure of PII or other protected information;

(2) Unauthorized access to, use of, or tampering with computer systems, including hacker attacks and denial of service, unless caused by a mechanical or electrical failure;

(3) Introduction of a computer virus or other malware;

(4) Response to any data breach; and

(5) Governmental agency or authority investigative or enforcement action as to data privacy and security or data breach matters.

Questions?* Please contact us.

Razvan E. Miutescu
rmiutescu@wtplaw.com
(410) 347-8744

* These slides are not intended to be a substitute for legal advice. Always seek experienced legal counsel to address risks based on your organization's own and unique circumstances.

Whiteford | Taylor | Preston LLP