Cybersecurity: Putting The Toothpaste Back In The Tube

Best Practices For Responding To A Security Breach
About us

Eleanor Vaida Gerhards

Michael J. Lockerby

Jason Adler
STOP WHAT YOU'RE DOING...

WE HAVE AN URGENT ANNOUNCEMENT!
YEAH, IF YOU'D GO AHEAD AND SILENCE YOUR CELL PHONE

THAT'D BE GREAT

https://memorygenerator.net/meme/238550
ROADMAP

I DON'T THINK IT MEANS WHAT YOU THINK IT MEANS
Get over it, can't put the toothpaste back in the tube. Just make wiser decisions in the future.
IMAGINE A WORLD
WHERE PEOPLE USED BEST PRACTICES
Definition of a Trade Secret

[1]nformation, including a formula, pattern, compilation, program, device, method, technique, or process, that:

(i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and

(ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

UTSA § 1(4)(1985)
- Safes
- Alarms
- Security personnel
- Photo identifications
- Use of locked cabinets
- Locked briefcases for transporting works
- Electronic sensors attached to documents
- Logging and identification of the materials
- Confidentiality agreements for all those given access
- Availability of the materials at only a handful of sites worldwide
Strategic Information

Hotel Central Reservation System
Computer Software Systems
Customer Information

Order History

<table>
<thead>
<tr>
<th>Order #</th>
<th>Order Date</th>
<th>Reference</th>
<th>Total</th>
<th>Ordered by</th>
<th>Preview of purchased items</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>15274775</td>
<td>22/03/2016</td>
<td></td>
<td>$59.25</td>
<td><a href="mailto:gardner@ccs.net.au">gardner@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice, Return</td>
</tr>
<tr>
<td>15274209</td>
<td>21/03/2016</td>
<td></td>
<td>$215.70</td>
<td><a href="mailto:gardner@ccs.net.au">gardner@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice, Return</td>
</tr>
<tr>
<td>15274208</td>
<td>21/03/2016</td>
<td></td>
<td>$730.40</td>
<td><a href="mailto:gardner@ccs.net.au">gardner@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice, Return</td>
</tr>
<tr>
<td>15274303</td>
<td>20/03/2016</td>
<td>NARESHOUSE 06/07</td>
<td>$370.03</td>
<td><a href="mailto:william@ccs.net.au">william@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15274309</td>
<td>20/03/2016</td>
<td>NARESHOUSE 06/07</td>
<td>$261.03</td>
<td><a href="mailto:william@ccs.net.au">william@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15275303</td>
<td>02/03/2016</td>
<td>PRINTERS</td>
<td>$1489.20</td>
<td><a href="mailto:clements@ccs.net.au">clements@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15275335</td>
<td>02/03/2016</td>
<td></td>
<td>$66.50</td>
<td><a href="mailto:paul@ccs.net.au">paul@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15275339</td>
<td>02/03/2016</td>
<td>PRINTERS</td>
<td>$91.25</td>
<td><a href="mailto:vildar@ccs.net.au">vildar@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15275388</td>
<td>02/03/2016</td>
<td>LEVEL 2 SUPPLIES</td>
<td>$135.68</td>
<td><a href="mailto:vildar@ccs.net.au">vildar@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
<tr>
<td>15276153</td>
<td>02/03/2016</td>
<td>OFFICE</td>
<td>$57.14</td>
<td><a href="mailto:cathy@ccs.net.au">cathy@ccs.net.au</a></td>
<td><img src="image" alt="Preview" /></td>
<td>Invoice</td>
</tr>
</tbody>
</table>
Recipes and Formulas

KFC
SECRET RECIPE
Methods of Operation, Processes, and Techniques
Prospective Franchisee Information
Product Line Extensions and Launch Dates
Supply Agreements
Top Sources of Data Breaches

<table>
<thead>
<tr>
<th>Trade Secret and Proprietary/Confidential Information</th>
<th>Third-Party Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rogue or Former Franchisees</td>
<td>Employees</td>
</tr>
<tr>
<td>Former Employees</td>
<td>Suppliers and Vendors</td>
</tr>
<tr>
<td>Competing Franchisors</td>
<td>Franchisees</td>
</tr>
<tr>
<td>Suppliers and Vendors</td>
<td>Third Party Bad Actors</td>
</tr>
</tbody>
</table>
Allocating Responsibility
Who do we Blame?

Trade Secret vs. Third Party Data Breach

• Franchisee?
• Supplier Vendor?
• Franchisor?
When it is the Franchisee’s Fault

• Shifting the financial responsibility for trade secret or third party cyber breaches does not necessarily mean shifting control over the clean-up
• Consider Blanket Master Cyber Insurance Policies vs. Individual Policies
• What does a Cyber Policy Cover/Not Cover?
When it is a Vendor’s Fault

Franchisor and franchisee vendors/suppliers are often a big source of cyber/data breaches and (almost) no one pays enough attention to this risk exposure.
Where Franchise Systems Go Wrong with Vendors/Suppliers . . .

• Due diligence
• Neglecting to carve out limits on liabilities/disclaimer of damages from standard boilerplate agreements
• Forgetting (in the case of third party breaches) **who owns the data, owns the response!**
Insurance in the Vendor/Supplier Context

Vendor Cyber Liability Policy
• Ensure the vendor’s cyber liability policy covers not only the loss of the vendor’s data but also the loss of the third party’s (franchisor’s) confidential/proprietary data/trade secrets

Vendor Errors and Omissions Policy
• Provides coverage for claims that a business acted negligently in providing services to customers
• Coverage for exposure can come from cyber and/or E&O

Franchisor’s Own Cyber Liability Policy
• Remember for third-party data breaches, franchisor remains data owner
• Coverage not available if vendor was bad actor in trade secrets claim
• No “offensive coverage” to go after misappropriating vendor
• Abatement coverage available in specific circumstances
When it is the Franchise System’s Fault

- Cyber Coverage
- Crime/Employee Theft Coverage
- Franchisor Error and Omission Coverage for lawsuits by franchisees against franchisor
- Shareholder Derivative Lawsuits
Implementing the Breach Response Plan

**COMPILE TEAM**
- CPO
- Trade Secrets Compliance Officer
- IT
- Counsel (In House and Outside)

**CONTAIN**
- Where is the Compromise?
- What is the scope?
- Is it over?
- Can it be Contained?

**CALL REINFORCEMENTS**
- Forensic Investigators
- Insurance Carriers
- Law Enforcement

**IDENTIFY BAD ACTOR**
- Cyber Criminal
- Franchisee
- Employee
- Vendor
Pre-Litigation Steps

**Preserve**
- Timeline
- Details
- Refresh
- Collection

**Notification**
- External Communications
- Victims

**Pre-Litigation Remedies**
- Cease and Desist
- Law Enforcement

**Litigation**
- UTSA – DTSA – CFAA – ECPA
- Computer Crimes Statutes
Attorney-Client Privilege Issues

- Educate IT and other Employees
- Work Product
- Avoiding Unnecessary Communications
- Anticipating Litigation
- Common Interest and Joint Defense Agreements
Litigation Options

- Is trade secret misappropriation *really* ≈ third party data breach?
- When to pursue judicial remedies?
- What remedies are available?
The missing link

• Same breach may expose *both* franchise system trade secrets and third party data
  • Supplier trade secrets
  • Franchisee trade secrets (*e.g.*, customer lists, financial reports)
  • Confidential customer personal information and financial data
Burden of proof

• Trade secrets: reasonable efforts to maintain secrecy
  • Disclosure agreements
  • Security precautions
  • Circumstances suggest disclosure prohibited
  • Whether information in public domain or “readily ascertainable”

• Third party data: reasonable efforts to maintain secrecy
  • Class actions, federal and state enforcement, actions, shareholder derivative suits
  • How “reasonable” if security for third party data not at least as stringent as security for company trade secrets?
Third party data breach

• Wyndham Worldwide
  • FTC enforcement
  • Class actions
  • Shareholder suits

• FTC allegations
  • Unreasonable data security practices”
  • Franchisor control made Wyndham liable for franchisees
Unreasonable security → franchisor liability

- Failed to limit access through readily available measures
- Improperly configured software resulted in storage of payment card information in clear text
- Inadequate franchisor information security policies
- Franchisor control of franchisees
Unreasonable security

- Failed to update servers with latest security patches
- Used default user IDs and passwords
- Failed to follow best practices for password complexity
- Failed to inventory computers on network

- Failed to employ reasonable measures to detect and prevent unauthorized access
- Failed to follow proper procedures to prevent repeated intrusions
- Failed to restrict third-party access to network
Franchisor control

- Required each franchisee to use designated computer system (property management system)
- PMS stored consumers’ personal information
- Administrator access
- Set rules for access
Remedies

• May be the same regardless of whether information accessed is (or was) a trade secret
• Access or posting may have destroyed trade secret status altogether
• Prompt pursuit may be only way to maintain trade secret status
Remedies

- Trade secret law
- CFAA
- Computer crimes laws
- ECPA
- Preliminary injunction
- Damages
- Costs & attorneys’ fees
- Sealing the record
When to pursue?

• Essential element of franchise system in jeopardy of being lost
• Posting on Internet threatens status
• Departing employees or franchisees using for competitor’s benefit
Consequences of posting on the Internet

• How long was it posted?
• How promptly did owner act?
• Who saw it?
• How accessible and popular are the Internet site?
• Where does it show up in response to search queries?
• How much was disclosed?
Preliminary injunction

- Warranted in cases of actual or threatened use or disclosure
- May be *only* remedy if no use or disclosure yet
  - Prohibitory injunction
  - Mandatory injunction requiring return of embodiments, assignment of patents, destruction
  - *Ex parte* seizure orders
Preliminary injunction

• Primary purpose to preserve “status quo”
  • “Last, actual peaceable uncontested status”

• Is “status quo” that trade secrets on the Internet, arguably gone?

• Computer crimes laws require no showing of trade secret protection

• Arbitration clause
  • What if no “carve-out” for preliminary injunctive relief?
  • Authority that federal courts can preserve status quo pending arbitration
  • Still good law now that most ADR rules authorize preliminary injunctive relief?
Practice pointers

• Seek expedited discovery, consolidation of trial and preliminary injunction hearing?

• Submit proposed order with findings and conclusions
  • “reasons for its issuance”
  • “be specific in terms”
  • “describe in reasonable detail ... the act or acts to be restrained”
    • Rule 65(d)
Practice pointers

• Make injunction binding on third parties pursuant to Rule 65(d)(2) “by service or otherwise”

• Remember that courts have considerable discretion over award and scope of injunctive relief

• May win or lose on “intangible” factors: reasonableness, credibility of witnesses, parties, counsel
Federal computer crimes

• Electronic Communications Privacy Act (ECPA)
  • Wiretap Act prohibits interception of communications
  • Stored Communications Act prohibits dissemination or review

• Computer Fraud & Abuse Act (CFAA)
CFAA damages

- Can include cost of forensic expert
  - “cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense”

- Some courts require showing “interruption of service”

- Statutory provision:
  - “any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service”
De-CFAA-nated?

• Ninth Circuit
  • CFAA provides no remedy against disloyal employees who retrieved confidential information via company user accounts and transferred it to competitor
  • Because defendants were authorized to access the computer, access for an unauthorized purpose was not “without authorization” and did not “exceed[] authorized access”
    • *U.S. v. Nosal*, 676 F.3d 854 (9th Cir. 2012)

• Fourth Circuit
  • CFAA provides no remedy against former employee who, before resigning, downloaded employer’s proprietary information at behest of competitor
  • WEC policies prohibited using information without authorization or downloading to PC but did not restrict Miller’s authorization to access the information
State computer crimes

- Prohibit “use” of computers “without authority”
- Typical remedies:
  - Sealing the record
  - Injunctive relief
  - Costs and attorneys’ fees
- Can combine with common law claim for “trespass to chattels”
State computer crimes

• Terminated dealer continued to access “dealers only” portal
  • Ordered to pay attorneys’ fees and cost of having forensic expert image and analyze computers in TN, AR, AL, and MS
  • *NACCO Materials Handling Group, Inc. v. The Lilly Co.*, 278 F.R.D. 395 (W.D. Tenn. 2011)

• Failure to disclose disabling code
  • Actionable under CFAA and Connecticut computer crimes law
    • *Roller Bearing Co. of Am., Inc. v. Am. Software, Inc.*, No. 3:07-cv-01516 (D. Conn.)

• Hacker reconstructed and sold customer list
  • *Ex parte TRO sealing record*
Pre-Incident Response Mitigation

“Information security is a big deal at my office so sometimes we have to communicate in code. We have 37 different symbols for the word ‘jerk’.”
Limit Risky Employee Conduct

**NOT SAFE**

- Using commercial email for work related tasks
- Posting files online because of email attachment size limitations
- Using i-Phones w/out password protection enabled
- Using Peer to Peer file sharing services
- Working with company materials on home computers
- Uploading franchise system proprietary information to the Cloud
- Copying sensitive information to unprotected portable devices ("thumb" or "jump" drive)
Saying Goodbye to the Cloud

- Employees may continue to have access after departure
- Dropbox and others can resist subpoenas
- Time and expense to get it back
- Evidence that a franchisee “failed to take reasonable measures” to protect data
- General security issues (susceptible to being hacked, stored and transmitted over internet, data leakage, loss of control over security measures)
Latest and Greatest for Employee Handbooks

- Need prior written permission from high-level IT person to download, duplicate, alter, remove, delete or install data files, passwords, and programs
- Strong password policy
- No sharing passwords
- Individualized and unique logins
- Fulsome social media policies for safe blogging/posting so as not to unintentionally disclose trade secrets
- On-board new employees with acknowledgements to avoid vicarious liability
- Make employees sign policies
Mitigating Losses at the Franchisee Level

- FRANCHISE AGREEMENT
- OPERATIONS MANUAL
- FRANCHISEE TRAINING
Dust off the Franchise Agreement

- Definition of IP
- Confidentiality
- Indemnification
- Insurance
- Franchisee Duties
- Definition of Customer Data
Balancing the Competing Forces

Natural adversity to involving in business operations at franchisee level due to increase risk of vicarious liability exposure but . . .

Where is it worth the risk and how?

TIPS -
Operations Manual
Initial and On-Going Training
Balancing the Competing Forces

Natural adversity to involving in business operations at franchisee level due to increase risk of vicarious liability exposure but. . .

Where is it worth the risk and how?
Balancing the Competing Forces

• Operations Manual
  • Forms
  • Best Practices
  • List Resources
• Initial and Ongoing Training
  • Merchant Services (PCI-DSS)
  • Approved Vendor Training
  • Recommended
• Do not allow facilitation of violations
• Do not allow franchisees to engage in insufficient data security practices
Franchise System Suppliers and Vendors

Risk Assessment

Due Diligence (privacy and security questionnaire)

Contractual Provisions

1. Audit Rights
2. Compliance with Laws
3. Indemnification for failure to maintain appropriate security measures
4. Minimum insurance limits
5. Carve out limits and caps for breaches of confidentially/data breaches
6. Notification
Electronic and Other Security Measures

- Shred, Destroy and Purge!
- Control Access
- Encrypt
- Move “Reply All” Button
- Prepare for attacks from the Outside
- Pre-Departure Investigations of Franchisees and Employees
- Exit Interviews with Franchisees and Employees
Questions and Answers

Any questions?
Anyone?
Anyone?