Technology & Compliance

Ted Banks • Heidi Rudolph • Gene Stavrou

SCCE Compliance and Ethics Institute
Breakout Session - October 21, 2018

About Us

Ted Banks

Heidi Rudolph

Gene Stavrou

About You
(A Quick Survey)

- Industry? Function/Department?
- Does your organization use social media to promote products or otherwise communicate with stakeholders?
- How has GDPR affected your organization?
- Does your organization have a Bring Your Own Device program?
- Has your organization lost assets or revenue due to malicious software or phishing attacks?

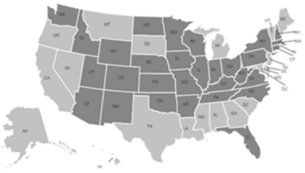
What We'll Cover in This Session

1. Role of CCOs and Compliance Personnel
2. Evolving Environment
3. Changing Technologies and Relevant Impacts
4. Real World Implications
5. Risk Assessment

1. Role of CCOs and Compliance Personnel

Compliance Must be More Involved in the Business

AMERICAN BAR ASSOCIATION
Center for
Professional Responsibility



> "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all [CLE] requirements to which the lawyer is subject." Ethical Responsibility of an Attorney. (*ABA Model Rule 1.1, Comment 8*)

31 States have formally adopted the revised comment to Rule 1.1

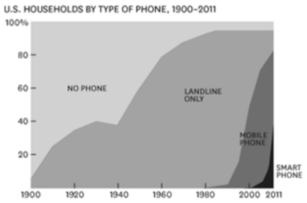
Source: https://www.lawsitesblog.com/tech-competence/

The ethical responsibility of an Attorney extends beyond substantive knowledge of a specific area of law.

Increasing Speed of Technology

Technology is being adopted at an increasing speed every year

FROM NO TELEPHONE TO SMART PHONES



SOURCE MICHAEL DEGUSTA AT THE MIT TECHNOLOGY REVIEW USING DATA FROM FORRESTER, KNOWLEDGE NETWORKS, NEW YORK TIMES, PEW, U.S. CENSUS

HBR.ORG

1987 20th Century Fox

"Alexa, what is blockchain?"

> *"…in 2005 Facebook didn't exist for most people, "twitter" was still a sound, the cloud was something in the sky, 3G was a parking space, applications were what you sent to colleges, and "Skype" was a typo."* –Thomas Friedman

2. Evolving Environment

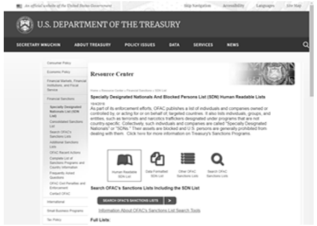
Trust and the Global Supply Chain

Sourcing is becoming more important than ever. In response to consumer interest, organizations are uncovering the sources of their products. This presents unique challenges that technologies like vendor management, third party diligence and blockchain are solving for.

The Grocery Manufactures Association estimates food fraud costs the global industry between $10-15b per year, affecting 10% of all commercially sold food products.

Compliance opportunity:

- Verify that business partners are not on SDN lists programmatically
- Investigate blockchain for smart contracts and provenance


An official website of the United States Government
Skip Navigation
Accessibility
Languages
Site Map
U.S. DEPARTMENT OF THE TREASURY
SECRETARY MNUCHIN
ABOUT TREASURY
POLICY ISSUES
DATA
SERVICES
NEWS
Consumer Policy
Economic Policy
Financial Markets, Financial Institutions, and Fiscal Service
Financial Sanctions
Specially Designated Nationals List (SDN List)
Consolidated Sanctions List
Search OFAC's Sanctions Lists
Additional Sanctions Lists
OFAC Recent Actions
Complete List of Sanctions Programs and Country Information
Frequently Asked Questions
OFAC Civil Penalties and Enforcement
Contact OFAC
International
Small Business Programs
Tax Policy
Resource Center
Home › Resource Center › Financial Sanctions › SDN List
Human Readable SDN List
Data Formatted SDN List
Other OFAC Sanctions Lists
Search OFAC Sanctions Lists
SEARCH OFAC'S SANCTIONS LISTS
>

Specially Designated Nationals And Blocked Persons List (SDN) Human Readable Lists

10/4/2018

As part of its enforcement efforts, OFAC publishes a list of individuals and companies owned or controlled by, or acting for or on behalf of, targeted countries. It also lists individuals, groups, and entities, such as terrorists and narcotics traffickers designated under programs that are not country-specific. Collectively, such individuals and companies are called "Specially Designated Nationals" or "SDNs." Their assets are blocked and U.S. persons are generally prohibited from dealing with them. Click here for more information on Treasury's Sanctions Programs.

Search OFAC's Sanctions Lists Including the SDN List

Information About OFAC's Sanctions List Search Tools

Full Lists:

Antitrust and Big Data

- Businesses use competitor’s public and private pricing data to drive their own pricing algorithms.
- If these algorithms result in non-competitive pricing, who is responsible?
- Is the person who developed and deployed the algorithm consciously committing an antitrust violations?

Data Privacy – European Union

- Comprehensive
- Focused on individual human rights
- Seven Principles:
  1. Lawfulness, fairness and transparency
  2. Purpose limitation
  3. Data minimization
  4. Accuracy
  5. Storage limitation
  6. Integrity and confidentiality (security)
  7. Accountability

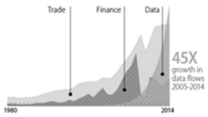
11 Key GDPR Tenets

1. Increases **the individual’s expectation** of data privacy and the organization’s obligation to follow established cybersecurity practices.
2. Establishes **hefty fines for non-compliance**. An egregious violation of GDPR, such as poor data security leading to public exposure of sensitive personal information, could result in a fine in the millions or even billions of dollars (there are two tiers of violations and the higher tier is subject to fines of over 20 million euros or 4% of the company’s net income).
3. Imposes detailed and demanding **breach notification requirements**. Both the authorities and affected customers need to be notified “without undue delay and, where feasible, not later than 72 hours after having become aware of [the breach]”. Affected companies in America that are accustomed to US state data breach reporting may need to adjust their breach notification policies and procedures to avoid violating GDPR.
4. Requires many organizations to appoint a **data protection officer (DPO)**. You will need to designate a DPO if your core activities, as either a data controller or data processor, involve “regular and systematic monitoring of data subjects on a large scale.” For firms who already have a chief privacy officer, making that person DPO would make sense, but if there is no CPO or similar position in the organization, then a DPO role will need to be created.
5. Tightens the definition of consent. **Data subjects must confirm their consent** to your use of their personal data through a freely given, specific, informed, and unambiguous statement or a clear affirmative action. In other words: silence, pre-ticked boxes, or inactivity no longer constitute consent.
6. Takes a **broad view of what constitutes personal data**, potentially encompassing cookies, IP addresses, and other tracking data.
7. Codifies a **right to be forgotten** so individuals can ask your organization to delete their personal data. Organizations that do not yet have a process for accommodating such requests will need to work on that.
8. Gives **data subjects the right to receive data** in a common format and to **ask that their data be transferred to another controller**. Organizations that do not yet have a process for accommodating such requests will need to work on that.
9. Makes it clear that **data controllers are liable for the actions of the data processors** they choose. (The controller-processor relationship should be governed by a contract that details the type of data involved, its purpose, use, retention, disposal, and protective security measures. For US companies, think Covered Entities and Business Associates under HIPAA.)
10. **Increases parental consent** requirements for children under 16.
11. **Enshrines “privacy-by-design”** as a required standard practice for all activities involving protected personal data. For example, in the area of app development, GDPR implies that “security and privacy experts should sit with the marketing team to build the business requirements and development plan for any new app to make sure it complies with the new regulation”.

Data Privacy – US

California, Massachusetts and Vermont have each passed regulations related to data privacy. Each has a different scope, and none are as broad as GDPR. Every state-level data privacy regulation strengthens the argument for harmonization at a federal level.

FTC: Inadequate privacy protection represents an unfair method of competition



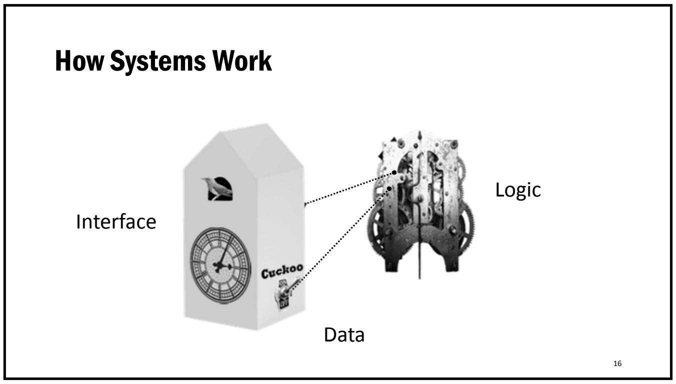
The volume of global data flows increased 45x from 2005 to 2014, growing faster than both international trade or financial flows[1]

[1] Digital Trade and U.S. Trade Policy, EveryCRSReport.com, May 2018

California Security of Connected Devices Law

- Takes effect January 1, 2020
- Governs any device capable of connecting to the internet (think IoT)
- Requires "reasonable security features" proportional to the device's "nature and function" and the "information it may collect, contain, or transmit"

3. Changing Technologies and Relevant Impacts



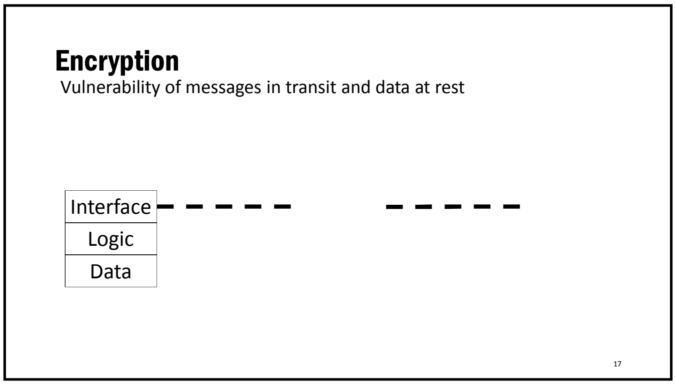
How Systems Work

Interface

Logic

Data

16

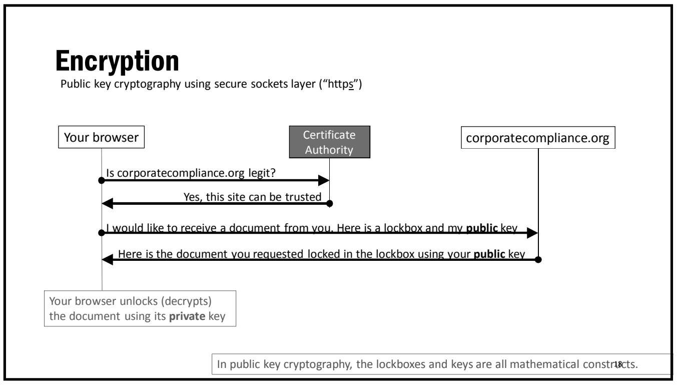


Encryption

Vulnerability of messages in transit and data at rest

Interface
Logic
Data

17



Encryption

Public key cryptography using secure sockets layer ("https")

Your browser

Certificate Authority

corporatecompliance.org

Is corporatecompliance.org legit?

Yes, this site can be trusted

I would like to receive a document from you. Here is a lockbox and my **public** key

Here is the document you requested locked in the lockbox using your **public** key

Your browser unlocks (decrypts) the document using its **private** key

In public key cryptography, the lockboxes and keys are all mathematical constructs.

18

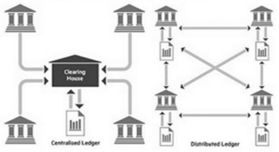
Blockchain

- Smart contracts
- Health records
- Voting systems

Legal Example:
Smart contract code within blockchain to track trademark/grey market products or spend funds only when a required percentage of people agree.

Embedding distributed ledger technology

A distributed ledger is a network that records ownership through a shared registry



In contrast to today's networks, distributed ledgers eliminate the need for central authorities to certify ownership and clear transactions. They can be open, verifying anonymous actors in the network, or they can be closed and require actors in the network to be already identified. The best known existing use for the distributed ledger is the cryptocurrency Bitcoin

FT graphic. Source: Santander InnoVentures, Oliver Wyman & Anthemis Partners

Conflicting forces:
GDPR and the right to be forgotten vs. Blocks of data that will live forever

Artificial Intelligence

- How are they building up AI?
- How will we deal with Automation of Jobs
- Aligns with the constant pressure to reduce headcount
  - Risk: Elimination of human control point

Organizations are using AI (artificial intelligence) for IA (intelligence augmentation)

Voice Activated Devices

- Legality – used as evidence in litigation
- Software updates, the way that they use data can change
- Always listening, how often are they recording?
  - State laws
- Lawyers: violation of ethical rules

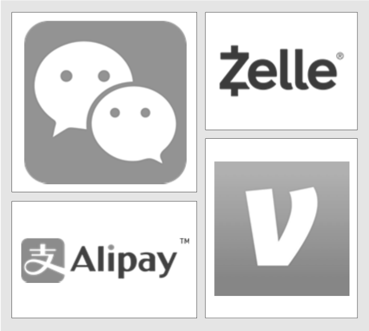
Welcome to May I accept a ...

Come back tomorrow to pla...

Thanks for opening May I ac...

Alright Have a great day!

https://getstoryline.com



Cashless Alternatives

- Auditable
- Security concerns
- Late development advantage

In Sweden, 2% of transactions are processed with cash, in the US 33% use cash.

Phishing

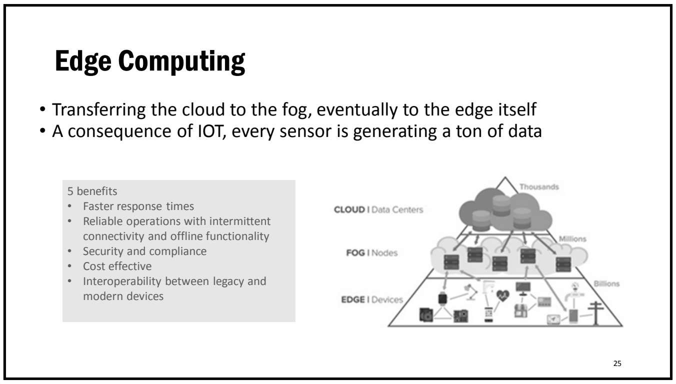
- Prevalence
- Sophistication
- Targeting
- Constant updates required

- Average cost of a phishing attach for a mid-size company - $1.6m
- 65% increase in phishing attacks in 2017[1]
- 30% of phishing messages get opened, 12% of those users click on the malicious attachment or link[2]
- 95% of all phishing attack on enterprise networks are the result of successful spear phishing[3]

[1] PhishMe’s Enterprise Phishing Resiliency and Defense Report
[2] Verizon Data Breach Investigations Report
[3] SANS Institute

Data ownership

- Giving control of data back to the original creator, instead of the platform
- Enterprise implications – businesses can share proprietary data without fear of theft or loss
- Fujitsu Data Exchange Network, IOTA Data Marketplace
- Privacy rules
  - Ease of clicking without reading
  - Backlash



Edge Computing

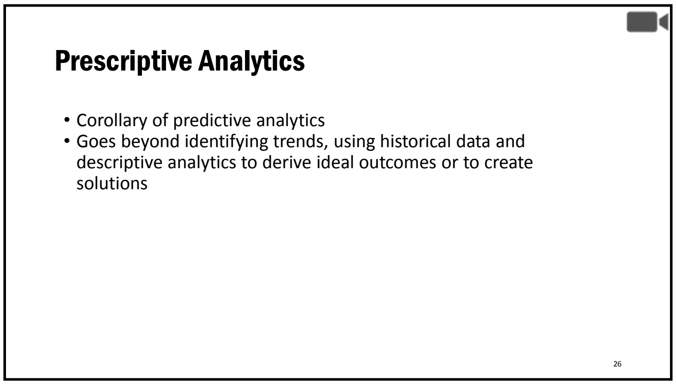
- Transferring the cloud to the fog, eventually to the edge itself
- A consequence of IOT, every sensor is generating a ton of data

5 benefits

- Faster response times
- Reliable operations with intermittent connectivity and offline functionality
- Security and compliance
- Cost effective
- Interoperability between legacy and modern devices

Thousands
CLOUD I Data Centers
Millions
FOG I Nodes
Billions
EDGE I Devices

25



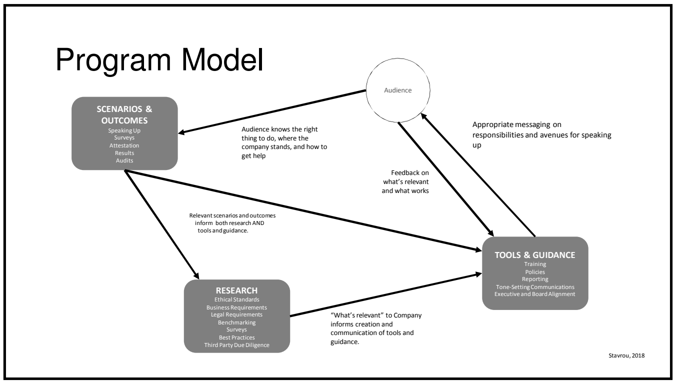
Prescriptive Analytics

- Corollary of predictive analytics
- Goes beyond identifying trends, using historical data and descriptive analytics to derive ideal outcomes or to create solutions

26

4. Real World Implications

27



Program Model

Audience

SCENARIOS & OUTCOMES
Speaking Up
Surveys
Attestation
Results
Audits

Audience knows the right thing to do, where the company stands, and how to get help

Appropriate messaging on responsibilities and avenues for speaking up

Feedback on what's relevant and what works

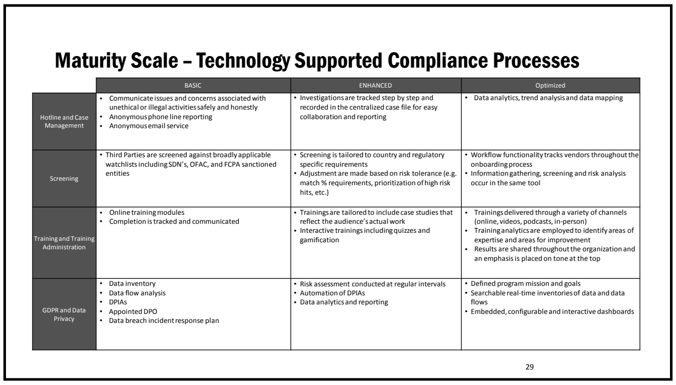
Relevant scenarios and outcomes inform both research AND tools and guidance.

TOOLS & GUIDANCE
Training
Policies
Reporting
Tone-Setting Communications
Executive and Board Alignment

RESEARCH
Ethical Standards
Business Requirements
Legal Requirements
Benchmarking
Surveys
Best Practices
Third Party Due Diligence

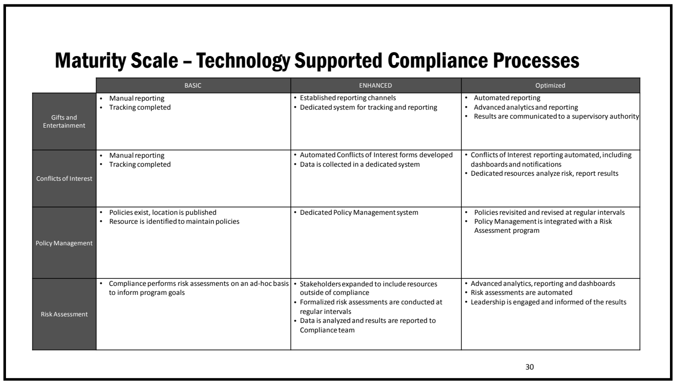
"What's relevant" to Company informs creation and communication of tools and guidance.

Stavrou, 2018



Maturity Scale – Technology Supported Compliance Processes

	BASIC	ENHANCED	Optimized
Hotline and Case Management	• Communicate issues and concerns associated with unethical or illegal activities safely and honestly • Anonymous phone line reporting • Anonymous email service	• Investigations are tracked step by step and recorded in the centralized case file for easy collaboration and reporting	• Data analytics, trend analysis and data mapping
Screening	• Third Parties are screened against broadly applicable watchlists including SDN's, OFAC, and FCPA sanctioned entities	• Screening is tailored to country and regulatory specific requirements • Adjustment are made based on risk tolerance (e.g. match % requirements, prioritization of high risk hits, etc.)	• Workflow functionality tracks vendors throughout the onboarding process • Information gathering, screening and risk analysis occur in the same tool
Training and Training Administration	• Online training modules • Completion is tracked and communicated	• Trainings are tailored to include case studies that reflect the audience's actual work • Interactive trainings including quizzes and gamification	• Trainings delivered through a variety of channels (online, videos, podcasts, in-person) • Training analytics are employed to identify areas of expertise and areas for improvement • Results are shared throughout the organization and an emphasis is placed on tone at the top
GDPR and Data Privacy	• Data inventory • Data flow analysis • DPIAs • Appointed DPO • Data breach incident response plan	• Risk assessment conducted at regular intervals • Automation of DPIAs • Data analytics and reporting	• Defined program mission and goals • Searchable real-time inventories of data and data flows • Embedded, configurable and interactive dashboards



Maturity Scale – Technology Supported Compliance Processes

	BASIC	ENHANCED	Optimized
Gifts and Entertainment	• Manual reporting • Tracking completed	• Established reporting channels • Dedicated system for tracking and reporting	• Automated reporting • Advanced analytics and reporting • Results are communicated to a supervisory authority
Conflicts of Interest	• Manual reporting • Tracking completed	• Automated Conflicts of Interest forms developed • Data is collected in a dedicated system	• Conflicts of Interest reporting automated, including dashboards and notifications • Dedicated resources analyze risk, report results
Policy Management	• Policies exist, location is published • Resource is identified to maintain policies	• Dedicated Policy Management system	• Policies revisited and revised at regular intervals • Policy Management is integrated with a Risk Assessment program
Risk Assessment	• Compliance performs risk assessments on an ad-hoc basis to inform program goals	• Stakeholders expanded to include resources outside of compliance • Formalized risk assessments are conducted at regular intervals • Data is analyzed and results are reported to Compliance team	• Advanced analytics, reporting and dashboards • Risk assessments are automated • Leadership is engaged and informed of the results

Uber

Was described as a “do whatever you have to do to get it done” environment.

Apple CEO Tim Cook threatened to have Uber’s iPhone app removed from the App Store in 2015, when it learned that the ride-sharing company had secretly found a way to identify individual iPhones, even once the app was deleted from the phone. (The New York Times)

Uber disclosed a 2016 data breach, affecting 57 million riders and drivers. As a result, their settlement with the FTC pertaining to data mishandling, privacy and security complaints dating back to 2014 and 2015 has been expanded to include 20 years of privacy audits.

Uber is the subject of a United States Department of Justice inquiry over a program that it used to deceive regulators who were trying to shut down its ride-hailing service. (The New York Times)

The Washington Post
Democracy Dies in Darkness

Business

The numbers are in, and #DeleteUber worked — in Lyft’s favor

By Abha Bhattarai
March 14, 2017

(Paul Sancya/AP)

Facebook

Last Year

Mueller focusing on Facebook posts in Russia probe

By Bob Fredericks September 13, 2017 | 2:22

MORE ON: RUSSIA

Facebook exec Sheryl Sandberg Russian ads should be released

Russia's attempts to sway American voters through Facebook are a "red-hot" focus of special counsel Robert Mueller's investigation into the election and possible links to President Trump's campaign, a new report said Wednesday.

This Year

BARRON'S

TECHNOLOGY | TECHNOLOGY TRADER

Facebook’s Newest Gadget After Data Breaches Takes Video Inside the Home

By David Marino-Nachison and Jon Swartz Oct. 8, 2018 2:06 p.m. ET Order Reprints Print Article

Facebook's new Portal device.

Text size

Here's our newest gadget! We promise it won't spy on you.

Tesla

Last Month

Elon Musk’s tweet about taking Tesla private has triggered a federal lawsuit

The SEC says Elon Musk should never run a public company again.

By Umair Irfan | Updated Sep 28, 2018, 9:23am EDT

This Month

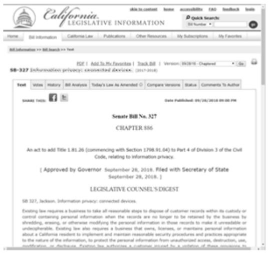
Tesla Tumbles After Musk Mocks SEC in Twitter Storm
Bloomberg
MUSK MOCKS SEC IN TWITTER STORM

IoT

2016

- In August 2016, a strain of malicious software detected 380,000 IoT devices still using unchanged, factory-set usernames and passwords.
- It used the devices to stage a Distributed Denial of Service attack, where certain servers were bombarded with requests from these devices, overburdening the servers and taking them down.

This Year



SB-327 Information privacy: connected devices. (2017-2018)

Date Published: 09/28/2018 09:00 PM

Senate Bill No. 327

CHAPTER 886

An act to add Title 1.81.26 (commencing with Section 1798.91.04) to Part 4 of Division 3 of the Civil Code, relating to information privacy.

[Approved by Governor September 28, 2018. Filed with Secretary of State September 28, 2018.]

LEGISLATIVE COUNSEL'S DIGEST

SB 327, Jackson. Information privacy: connected devices.

Existing law requires a business to take all reasonable steps to dispose of customer records within its custody or control containing personal information when the records are no longer to be retained by the business by shredding, erasing, or otherwise modifying the personal information in those records to make it unreadable or undecipherable. Existing law also requires a business that owns, licenses, or maintains personal information about a California resident to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure. Existing law authorizes a customer injured by a violation of these provisions to

Theranos

Inc.
HOW TO BUILD A COMPANY TO LAST 100 YEARS
THE NEXT STEVE JOBS
8 WOMEN WHO COULD OWN THE FUTURE
DO YOU REALLY

- Board of Directors – “Never occurred to ask”
  - Do board members understand technology?
- How could they have gotten ahead of this?
- Role of attorneys in compliance:

Cybersecurity

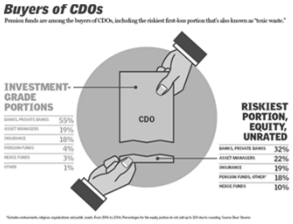
- Must run analysis periodically.
- Risk: Penetration by bad guys to capture data, extract ransom
  - Review: policies, network protection, data protection, anti-malware, auditing, monitoring, detection, use of mobile devices
  - Contingency planning?
  - Third-party risks
- Awareness and training
- More specific rules
  - New York Cybersecurity Requirements for Financial Services Companies, 23 NYCRR 500
  - SEC disclosure rules for cyber risks and incidents, 17 CFR 229, 249

The Board and Cybersecurity

1. Do they understand technology structure of company and risks?
2. Is there a technology expert or tech. board committee? (audit committee not sufficient)
3. Have the board members taken cybersecurity training or participated in a breach simulation?
4. Is there a *Silicon Valley* scenario: We're not selling a product, we're selling the stock price

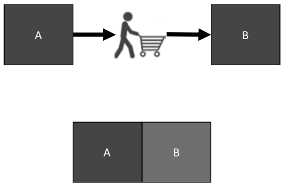
2008 Financial Crisis

- Convoluted instruments went beyond most people's understanding
- How could we have gotten ahead of this?
- Never approve anything you don't understand: Enron



Understand Your Process

- Factory gets new facility, removes the need for an old man to take the batch of chocolate across the floor, inadvertently changes consistency of chocolate
- How do you maintain high levels of customer service, quality control and risk management when automating?



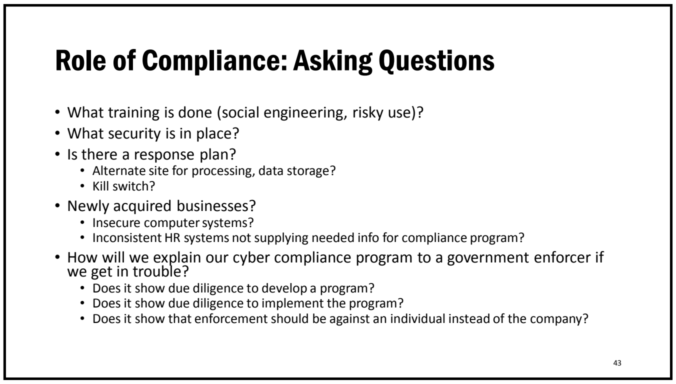
5. Risk Assessment

Compliance Program Measurement

5 Essential Elements of Compliance	DOJ Compliance Program Evaluation 2017	US Revised Federal Sentencing Guidelines, Chapter 8, 2012	UK Bribery Act of 2010
Tone, leadership and messaging that includes an unambiguous, visible and active commitment to compliance; the Board must ensure compliance policies, systems and procedures in place	Commitment from senior and middle management, including clear messaging against corruption	-Governing authority with knowledge and oversight -Designated high-level personnel assigned responsibility for program -Designated individuals with day to day responsibility and adequate resources/authority	Top level commitment to confront bribery
Risk assessments designed to provide a big picture of overall compliance obligations and identify areas of high risk to prioritize resources	Risk assessment process in place with regular information gathering and analysis and remediation	Organization responds to criminal conduct	Periodic risk assessment that considers internal and external risk
Standards and controls including 1) Code of Conduct; 2) Standards and Policies; and 3) Procedures	-Code of conduct and compliance policies and procedures -Incentives and disciplinary measures -Third party due diligence and payments -Mergers & acquisitions diligence	-Standards & procedures to prevent and detect criminal conduct -Promote ethics and compliance through incentive and disciplinary programs	-Proportionate procedures to prevent risk -Risk based due diligence
Training and communication with focus on training the right people with appropriate risk level consideration	Risk-based training tailored for high-risk and control employees; analysis to determine who should be training and on what subjects Communications regarding misconduct	Communication and training	Communications (including training); policies and procedures are embedded and understood; training proportionate to the risk
Oversight to ensure employees are adhering to the compliance program	-Analysis and remediation of underlying misconduct -Autonomy and resources -Confidential reporting and internal investigation -Continuous improvement, periodic testing and review	-Evaluate effectiveness -Reporting without fear of retaliation	Evaluate the effectiveness of procedures and adapt where necessary

Technology Risk

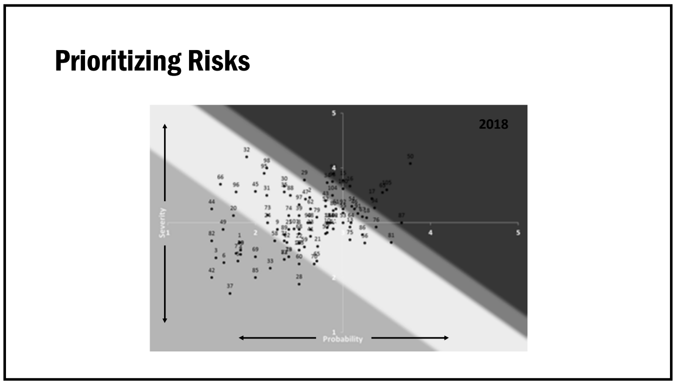
- Compliance must have a seat at the table
  - Competing interests across the organization
  - Communication is paramount
- Think about all of the ways that new technology can expose company
  - Are functions legal? (specific regulations from FTC, FDA, etc.)
  - What if data breach?
  - Reduction of product/service quality?
  - Cost to remediate?
  - Covered by insurance?
  - Privacy?
  - Rejection by customers?
  - Constant monitoring and updating to deal with new threats?



Role of Compliance: Asking Questions

- What training is done (social engineering, risky use)?
- What security is in place?
- Is there a response plan?
  - Alternate site for processing, data storage?
  - Kill switch?
- Newly acquired businesses?
  - Insecure computer systems?
  - Inconsistent HR systems not supplying needed info for compliance program?
- How will we explain our cyber compliance program to a government enforcer if we get in trouble?
  - Does it show due diligence to develop a program?
  - Does it show due diligence to implement the program?
  - Does it show that enforcement should be against an individual instead of the company?

43



Prioritizing Risks

Enjoy the rest of the conference!

Ted Banks
tbanks@scharfbanks.com

Heidi Rudolph
heidi.rudolph@moraeglobal.com

Gene Stavrou
gene.stavrou@ingredion.com