# Cybersecurity:

## A Practical Application

Louisiana State Bar Association
COVID Series CLE

**May 19, 2020**

David V. Meyer, Esq. MBA CISSP

Chief Information Security Officer
Financial Risk Mitigation, Inc.
law@davidvmeyer.com
504-931-1580

LA Bar # 37800
CISSP License # 484872

Chair: LSBA Cybersecurity Seminar (2019)
Lecturer for LSBA,LADB, ACFE, and IIA

Veterans Law, Int'l Privacy Law, and Cyber Ethics

BS, Information Systems and Decision Sciences: 2002
JD, Loyola College of Law: 2006
MBA, Louisiana Tech University: 2011

Certified Information Systems Security Professional (CISSP)
IT Consultant for over 25 years
Member, FBI InfraGard - Financial Services Sector

# Overview

1. Sources of Cybersecurity requirements
2. “Define your perimeter” best practices
3. You are your own worst enemy
4. Cloud
5. Disaster Recovery
6. Logging
7. Third-party independent review
8. Insurance
9. Checklist

# 1. Sources of Cybersecurity Requirements

- Model Rule 1.6(c) – “reasonableness” requirement.
- Model Rule 5.3 – duty of supervision over non-lawyers.

- ABA Formal Opinion 477 - the intersection of three bedrock ethical duties: competence, communication, and confidentiality.

- Statute: HIPPA, HITECH, 17 CFR 248.30, etc.
- NYS Dept. of Financial Services Cybersecurity Regulation.

- Contract or Nature of the information.

- **Vendor Due Diligence** – becoming more frequent.

# 1. Sources of Cybersecurity Requirements

LA R.S. 51:3074(A) (2018):

- "**Any person that conducts business in the state** or that owns or licenses computerized data that **includes personal information**, or any agency that owns or licenses computerized data that includes personal information, **shall 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."

LA R.S. 51:3073 (4)(a)(i)-(v) (2018):

"Personal information" means the first name or first initial and last name of an individual resident of this state in combination with any one or more of the following data elements, when the name or the data element is not encrypted or redacted:

- (i) **Social security number**.
- (ii) **Driver's license number** or state identification card number.
- (iii) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's **financial account**.
- (iv) **Passport number**.
- (v) Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as fingerprints, voice print, eye retina or iris, or other unique biological characteristic that is used by the owner or licensee to uniquely authenticate an individual's identity when the individual accesses a system or account.

# 1. Sources of Cybersecurity Requirements

Client Management: **Cybersecurity Assessments** *of your firm*

"Outsourced relationships should be subject to the same risk management, security, privacy, and other policies that would be expected if the financial institution [Client] were conducting the activities in-house."

– FFIEC IT Examination Handbook

Examples - Certain regulators have specific guidance for cybersecurity oversight in a vendor management context:

"Third Party Risk: Guidance for Managing Third Party Risk," **FDIC** FIL-44-2008, June 6, 2008;

**OCC** Bulletin 2013-29, "Third-Party Relationships: Risk Management Guidance," Oct. 30, 2013;

**Federal Reserve Board** Supervision and Regulation Letter 13-19 "Guidance on Managing Outsourcing Risk," December 5, 2013;

**FinCEN** Advisory FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime," October 25, 2016.

# 1. Sources of Cybersecurity Requirements

International cybersecurity regimes are often much stronger than similar regulations in the United States:

**EU GDPR** (May 25, 2018);

**German Federal Data Protection Act** (BDSG) IT Security Act (ITSG) (2015); and

**PRC Cybersecurity Law** (June 1, 2017).

# Answer: Cybersecurity Frameworks and Experts

- **ISO/IEC 27002(2013)** – recommended.
- PCI DSS – payment card transactions, limited use.
- NIST Pub. 800-53 – narrow, but useful.

**“Any lack of individual competence by a lawyer to evaluate and employ safeguards to protect client confidences may be addressed through association with another lawyer or expert, or by education.”** Model Rule 1.1 cmts [2] & [8] (2016).

Something cool:

# Global Cyber Attack Map

- "Digital Attack Map" is a live data visualization of DDoS attacks around the globe:

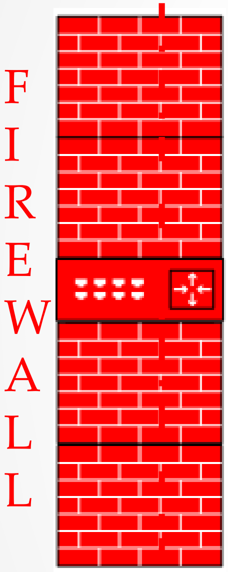
http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&list=0&time=17728&view=map

Notes:

- The visualization is only for a certain type of attack called "DDoS."
- These types of attacks will only grow in frequency.

# 2. Define your perimeter

The Firewall is the **most important** cybersecurity tool because it is the first line of defense. As a result, examine the following functionality when considering the firewall in your environment:



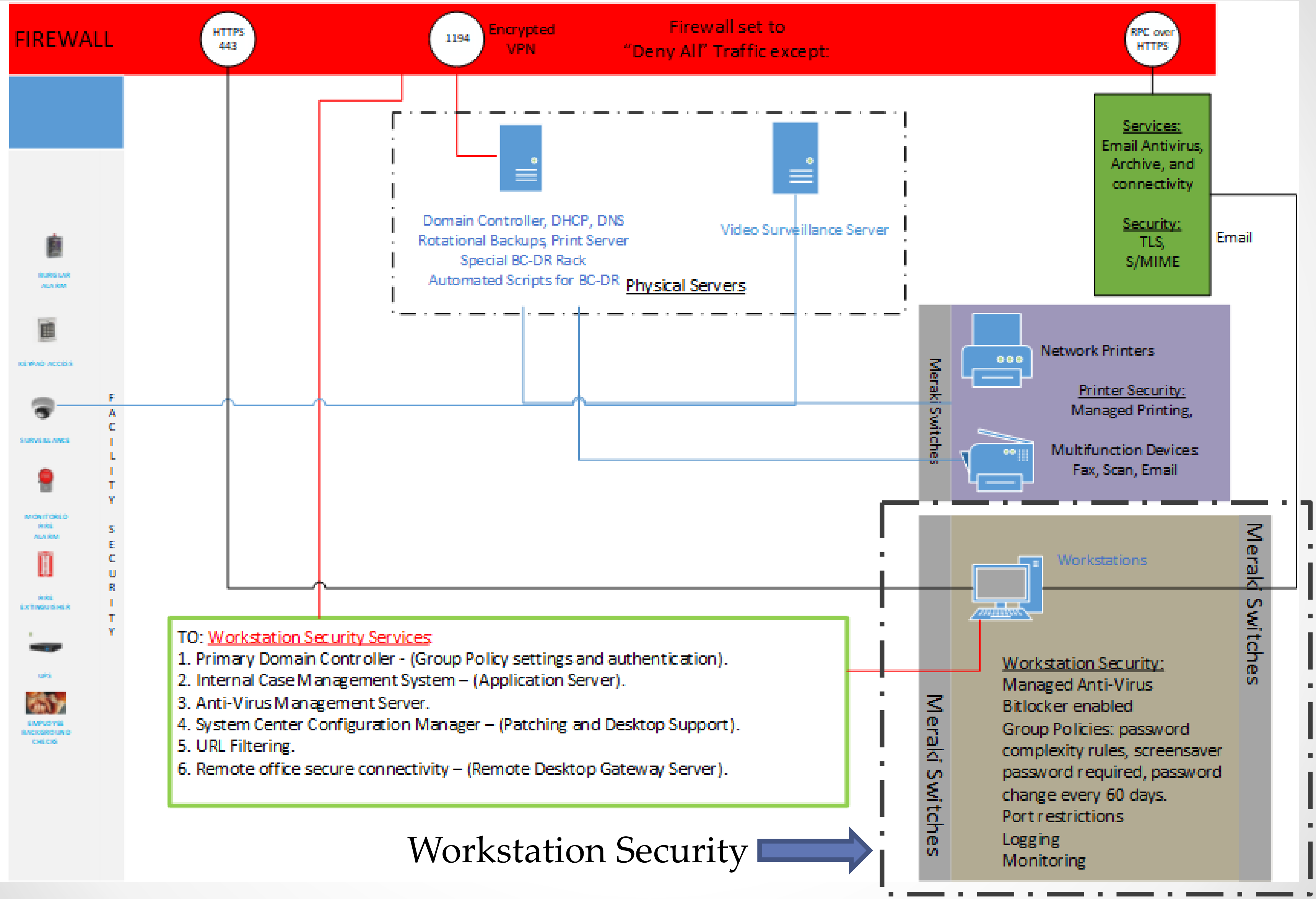
- Purchase a subscription to automatically update both "signatures" and "definitions."
- Commercial-grade firewalls with IPS/IDS capability are reasonable in a law practice **of any size**, except perhaps some solo practitioners (unless a client or contract says otherwise).
- Filter Internet traffic to exclude certain sites and "categories" of sites, including the capability to provide "packet inspection" functionality to examine HTTPS traffic.*
- Do not exempt any User from the filtering policy simply because the User is an attorney or owner of the firm; security posture is weakened by granting exemptions.
- Use alert functionality to notify an Administrator about issues (not updated, not filtering, malicious activity) that also establishes a testing procedure to confirm that updates are installed, that traffic is blocked, that no one is exempt, and that alerts are working.
- Set the Firewall to "Deny All" connections and then crawfish backwards to allow only those connections that are a business requirement.

Public Internet

Internal Network

*Packet Inspection is key as more sites transition to secure HTTPS connections (the green padlock).

# Sample Network Topology Diagram (mid-size Firm):



FIREWALL

HTTPS 443

1194 Encrypted VPN

Firewall set to "Deny All" Traffic except:

RPC over HTTPS

Services:
Email Antivirus, Archive, and connectivity

Security:
TLS,
S/MIME

Email

Domain Controller, DHCP, DNS
Rotational Backups, Print Server
Special BC-DR Rack
Automated Scripts for BC-DR

Video Surveillance Server

Physical Servers

Meraki Switches

Network Printers

Printer Security:
Managed Printing,

Multifunction Devices
Fax, Scan, Email

Workstations

Workstation Security:
Managed Anti-Virus
Bitlocker enabled
Group Policies: password complexity rules, screensaver password required, password change every 60 days.
Port restrictions
Logging
Monitoring

Meraki Switches

Meraki Switches

BURGLAR ALARM

KEYPAD ACCESS

SURVEILLANCE

MONITORED FIRE ALARM

FIRE EXTINGUISHER

UPS

EMPLOYEE BACKGROUND CHECKS

FACILITY SECURITY

TO: Workstation Security Services
1. Primary Domain Controller - (Group Policy settings and authentication).
2. Internal Case Management System – (Application Server).
3. Anti-Virus Management Server.
4. System Center Configuration Manager – (Patching and Desktop Support).
5. URL Filtering.
6. Remote office secure connectivity – (Remote Desktop Gateway Server).

Workstation Security

# 3. You are your own worst enemy

Humans are the greatest threat to any organization:

- Do not exempt any User from security measures simply because the User is an attorney or owner of the firm.
- Remain vigilant at all times because bad actors do not take a break.

Written Policies and Procedures for cybersecurity are mandatory:

- Provides cover in case of a security incident or breach.
- Review the Policies and Procedures at least annually.
- Acceptance of the review must also occur and be documented.
- Constant improvement of the Policies and Procedures shows awareness of and respect for cybersecurity measures and regulatory mandates.
- Provides clear guidance when an incident or breach occurs.

Security Awareness Training must be mandatory:

- At least annually, conduct training on common threat vectors, such as phishing emails, Social Engineering attacks, or sharing passwords; record your training methods and participant names for future reference (Sony 2014; Bangladeshi bank 2016;WannaCry 2017) and for evidence that the training actually occurred.

# 3. You are your own worst enemy, cont'd

## No wireless, NO wireless, NO WIRELESS

There is never a business case for having wireless access in your office. Wireless is a luxury to you, a courtesy to visitors, and an easy vector.

## Password Manager

Using the same password for every login credential is setting up failure. Use a secure and trusted password management application to record your credentials in a single space (e.g. Norton Password Manager).

Admin access: QuadrigaCX (Canada), cryptocurrency loss 2019.

## Ethical Hackers

Hire a white-hat ethical hacker service to perform "network penetration testing" on your internal network and any public-facing web applications at least once per year, and after major network infrastructure changes (*See also* Topic #7 – Third-Party Independent Review.)

Cybersecurity often gets a backseat to business demands, but that has to change. **Cyber risk is firm risk and attorney risk**.

# 3. You are your own worst enemy, cont'd

LSBA Ethics Advisory Service:

**"Lawyer's Use of Technology" (2019)**

Public Opinion 19-RPCC-021

https://www.lsba.org/documents/Ethics/EthicsOpinionLawyersUseTech02062019.pdf

Free service providing confidential non-binding advice regarding the LA Rules of Professional Conduct.

ABA Formal Opinion 483 - October 17, 2018: "Lawyer's Obligations After an Electronic Data Breach or Cyberattack"

https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/aba_formal_op_483.pdf

October 29, 2016 - "The Dinosaur in the Park" (Canada)

https://lawprofessors.typepad.com/legal_profession/2016/10/an-attorneys-inability-to-adjust-to-modern-law-technological-practice-was-allowed-to-surrender-his-license-in-a-proceeding-be.html

March 30, 2016 - "Illiteracy as Mitigation" (Oklahoma)

https://lawprofessors.typepad.com/legal_profession/2016/03/a-technology-challenged-attorney-admitted-in-1968-has-been-censured-by-the-oklahoma-supreme-court-for-misconduct-before-a-uni.html

# 4. Cloud

## Benefits:

- Offsite secure and redundant storage of client information, including working from home when required.
- Disaster recovery aide.
- Reduced capital expenditures on physical server equipment and maintenance by converting to an operating expense.

## Risks:

- Mistakenly-configured storage buckets that expose confidential client information to the world (RNC 2017); Virgin Media (2020)
- Lax administrator oversight (what is your IT team doing?); Capital One (2019).
- Exposed perimeter endpoints that are unsecured through vendor relationships (Home Depot 2015, General Electric 2020).
- Capital One (2019) internal user accessed Amazon S3 buckets.
- Carnival Cruise Lines (2020) employee email social engineering attack.
- Ownership and Destruction of the information.

## Encryption:

- Encrypting cloud infrastructure where confidential client information is stored is required, including encryption when transmitting the information and when the information is at rest.
- Encryption Key Management practices must be sufficient.

# 5. Disaster Recovery

Attorneys must be aware of the risks associated with living in S. Louisiana (predominantly hurricanes), but other threats must also be considered: hazmat, pandemic flu, fire.

ABA Formal Opinion 482 (Sept. 19, 2018) – attorney duties during disasters.

Different "disasters" have different responses, e.g. digital end of life, credentials management: crypto currency exchange head died and didn't tell anyone the password. https://mashable.com/article/quadrigacx-sent-bitcoin-to-inaccessible-cold-wallet/#HlvWvw.faaqi

Whatever your DR Plan, take these steps:

- Test it at least once per year and record the result; stumbling blocks and improvements should be noted and implemented.
- Write it down and disseminate to all employees.
- Review the testing results in preparation for next year.

Have a "Plan B"

Example: Houston was the primary dedicated evacuation and reconstitution site, but Hurricane Harvey forced immediate reconsideration and re-evaluation for alternative.

# 6. Logging

LA RS 51:3071: the affected entity must conduct a "reasonable investigation in order to determine the scope of the breach and to restore the reasonable integrity of the data system."

Log events are generated by the tens of thousands every hour; filtering which log events are relevant is key to determine security vulnerabilities.

99% of log events are irrelevant because the events are merely "informational" indicating that "something happened."

Relevant log events include:

- Logon attempts, whether successful or unsuccessful, can indicate attempted access to unpermitted information (breach?).
- Status updates of perimeter defense and internal controls.

Filter log events with "critical" or "high" status to an email address for alerting and remediation tracking through to completion.

- Ignore (but save) the noise to gain visibility into what's happening under the hood and behind the scenes.

Something cool:

# The Dark Web

- A visualization of data flow on the TOR network (each relay is placed on a world map and traffic exchanged between relays is indicated by animated dots):

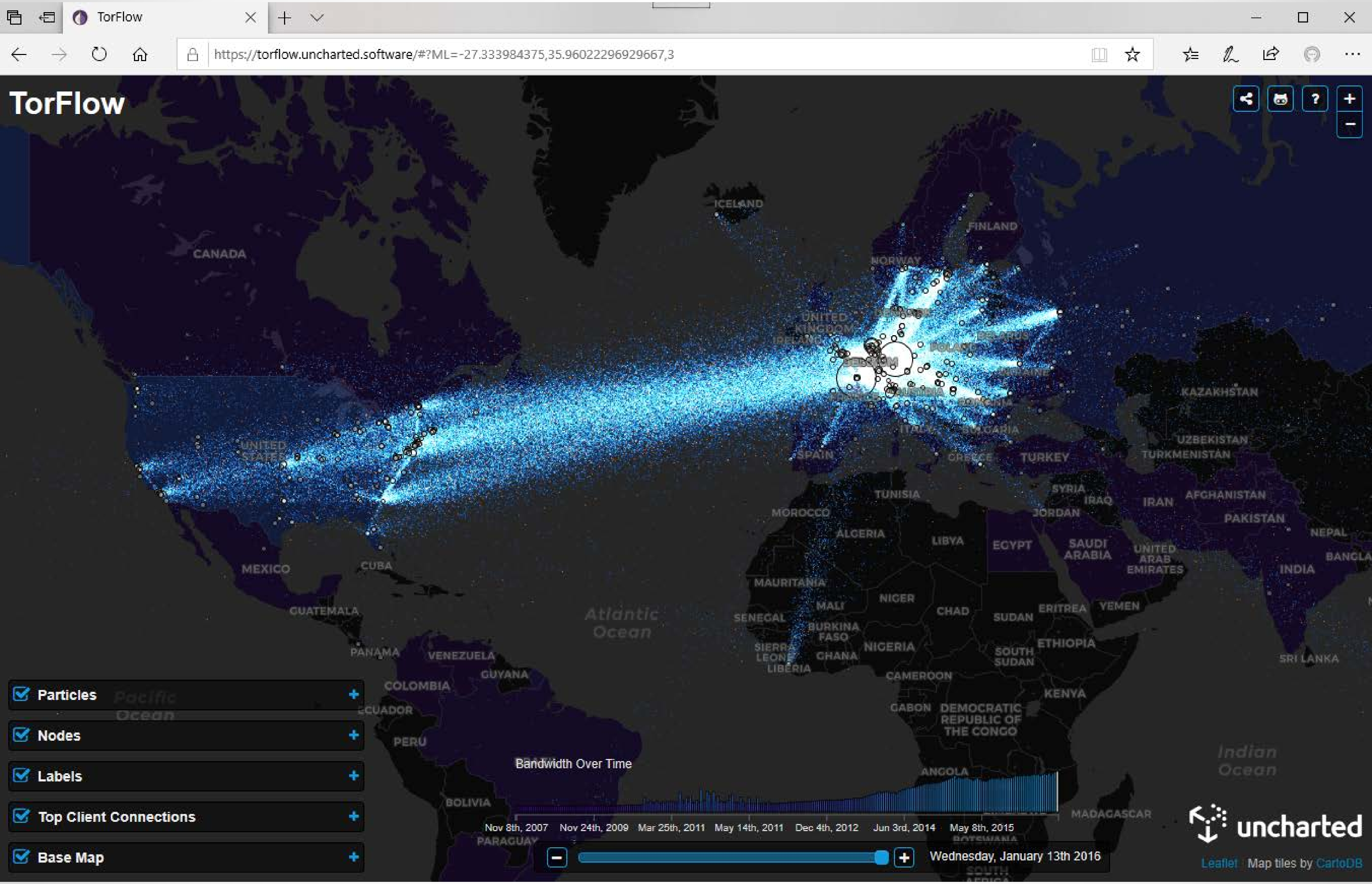
https://torflow.uncharted.software/

Notes:

- You cannot “accidentally” get onto the Dark Web.
- Never attempt to access the Dark Web.

https://www.cnbc.com/2018/07/11/hackers-selling-access-to-law-firm-networks-on-dark-web-sites.html

# The Dark Web



TorFlow
https://torflow.uncharted.software/#?ML=-27.333984375,35.96022296929667,3
TorFlow
☑ Particles +
☑ Nodes +
☑ Labels +
☑ Top Client Connections +
☑ Base Map +
Bandwidth Over Time
Nov 8th, 2007
Nov 24th, 2009
Mar 25th, 2011
May 14th, 2011
Dec 4th, 2012
Jun 3rd, 2014
May 8th, 2015
Wednesday, January 13th 2016
uncharted
Leaflet
Map tiles by CartoDB
CANADA
UNITED STATES
MEXICO
CUBA
GUATEMALA
PANAMA
VENEZUELA
GUYANA
COLOMBIA
ECUADOR
PERU
BOLIVIA
PARAGUAY
Pacific Ocean
Atlantic Ocean
ICELAND
FINLAND
NORWAY
UNITED KINGDOM
IRELAND
BELGIUM
POLAND
BELARUS
UKRAINE
ROMANIA
BULGARIA
ITALY
SPAIN
GREECE
TURKEY
KAZAKHSTAN
UZBEKISTAN
TURKMENISTAN
SYRIA
IRAQ
IRAN
AFGHANISTAN
PAKISTAN
NEPAL
INDIA
JORDAN
TUNISIA
MOROCCO
ALGERIA
LIBYA
EGYPT
SAUDI ARABIA
UNITED ARAB EMIRATES
MAURITANIA
MALI
NIGER
CHAD
SUDAN
ERITREA
YEMEN
SENEGAL
BURKINA FASO
NIGERIA
GHANA
SIERRA LEONE
LIBERIA
ETHIOPIA
SOUTH SUDAN
CAMEROON
KENYA
GABON
DEMOCRATIC REPUBLIC OF THE CONGO
ANGOLA
MADAGASCAR
BOTSWANA
SOUTH AFRICA
SRI LANKA
Indian Ocean

# 7. Third-party Independent Review

Some regulators (OCC, FinCEN, Treasury) require an independent review of the cybersecurity posture surrounding your network:

- The “independence” of the reviewer is the key, like an auditor.
- Performed in-house or by a contractor, as long as the reviewer can effect change based on the results of the review.
- ISO 27001(2013) is a recommended standard, but others are also available that may be a better fit (or required by statute or required by contract or the nature of the information).

Review the firewall at least annually to confirm you are locked-down tight. Hire ethical hackers to perform penetration testing.

**Client Assessments** ask whether a 3rd-party audit is performed *on your firm*, so get ready to respond to these assessments sooner rather than later:
ABA Journal, August 2018: http://www.abajournal.com/magazine/article/clients_outside_counsels_cybersecurity

# 8. Insurance

Box the remaining risk with a cyber insurance policy.

Examine the policy closely for exclusions based on different types of cyber attacks or fact scenarios:

- Social Engineering versus Brute Force attacks.
- Improperly-configured perimeter defenses (Target 2013).
- Improperly-configured internal controls (Capital One 2019).
- Uninstalled updates to defenses that you knew or should have known were not deployed (Equifax, 2017; Mossack Fonseca, 2016).

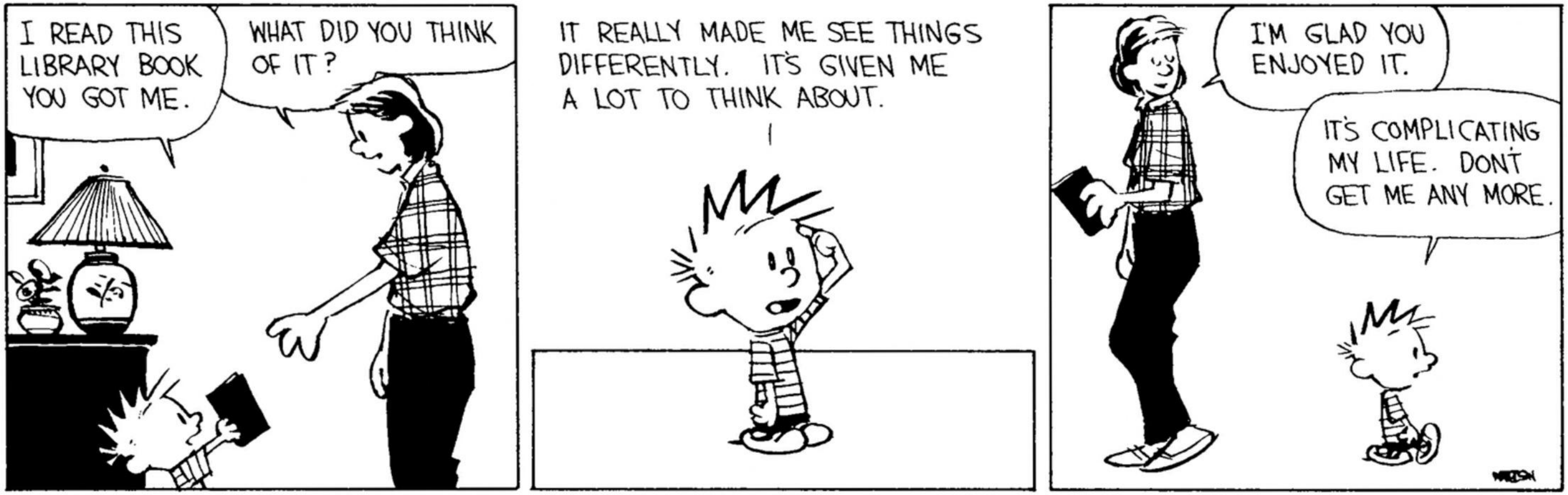
Include certain riders based on business need or risk:

- Incident Response and Breach Notification Assistance, Infiltration Identification and Remediation Assistance, and Privacy Assistance.
- Insurer may have readily-available access to helpful resources.

Law Enforcement contacts show that you take cyber security seriously.

# 9. Checklist

- ❑ Firewall: commercial-grade; subscription to auto-update signatures and definitions; website filtering; packet inspection.
- ❑ No Users are exempt from security policy.
- ❑ Policies and Procedures are written and reviewed.
- ❑ Security Awareness Training performed at least annually.
- ❑ Remove wireless access from the environment.
- ❑ Secure password manager software program/application.
- ❑ Hire ethical hackers to perform penetration testing yearly.
- ❑ Cloud: review storage bucket configurations, use encryption as much as possible, and adequate key management.
- ❑ Disaster Recovery: write it down, review it annually, Plan B.
- ❑ Logging: enable it, capture it, filter it, review it, document it.
- ❑ Insurance: get a Cyber Liability policy with necessary riders.
- ❑ Third-party review of: firewall rules; Policies and Procedures; Disaster Recovery Plan; network penetration; and logging.


I READ THIS LIBRARY BOOK YOU GOT ME.
WHAT DID YOU THINK OF IT?
IT REALLY MADE ME SEE THINGS DIFFERENTLY. IT'S GIVEN ME A LOT TO THINK ABOUT.
I'M GLAD YOU ENJOYED IT.
IT'S COMPLICATING MY LIFE. DON'T GET ME ANY MORE.
WATSON