



# **Volunteer Leadership Institute - Hawaii**

## **MITIGATING CYBER LIABILITY**

---

**Sarah Anderson**

*Founder & Attorney, SWA Law LLC, dba LegallyCyber.com*

### **Learning Objectives**

1. Identify and mitigate administrative risks to digital infrastructure through corporate policy.
2. Identify and understand data security compliance requirements under the Gramm-Leach Bliley Act Safeguards Rule.
3. Identify minimum network standards to mitigate risk of civil liability.
4. Identify and procure minimum coverage items to maximize cyber insurance benefits.



# MITIGATING CYBER LIABILITY

January 2025



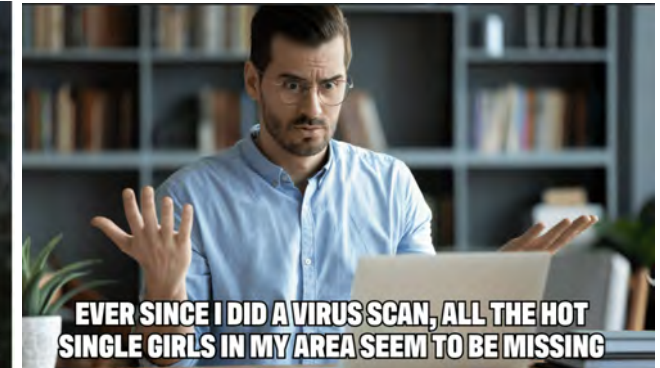
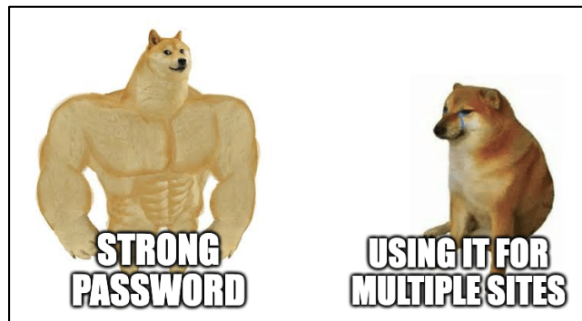
**SWA**  
LAW LLC



# THEME

## Cybersecurity is a mess. Just do your best.

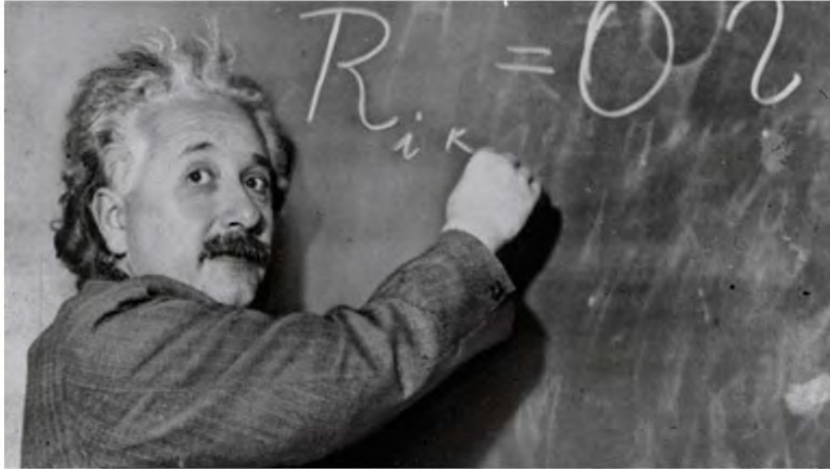
Employees when their CEO starts talking about the Rhymetec vCISO like they're an actual co-worker.





# AGENDA

How I think I look explaining cyber risk to the board



How I actually look



- **Common Misconceptions**
- **Threat Actor Motivations**
- **Administrative Risk Mitigation**
  - The Trinity of Cyber Risk Mitigation
  - Administrative Policy Goals
  - Mandatory Administrative Policies
  - Network Security/Acceptable Use
  - Third Party Risk Management
- **Compliance Requirements**
  - Regulated Data
  - New State A.I. Laws
  - GLBA
  - Cybersecurity Compliance
  - Keys to Legal Compliance
- **Navigating Cyber Insurance**
  - Shopping and Apply for Coverage
  - 3 Post-Incident Trips for Insured
- **Emerging Threats**
  - Cookie Theft
  - New Phishing Attacks



# COMMON MISCONCEPTIONS

*"My organization is so small, no one would target us."*

*"We don't have any valuable intellectual property on our systems."*

*"We are entirely cloud-based and the application encrypts our data in the cloud."*

*"We have back-ups and insurance, so we are not very concerned about cyber events."*

**"If it did happen, we just wouldn't tell anyone."**



# COMMON MISCONCEPTIONS



“My organization is so small, no one would target us.”

- ***Correction: Bad actors will target you because you are small. It's easy to them.***

“We don't have any valuable intellectual property on our systems.”

- ***Correction: Bad actors do not pick targets exclusively because of intellectual property. Many just cast a wide-net for victims, indiscriminately to see what value, of any kind that can be extorted.***

“We are entirely cloud-based and the application encrypts our data in the cloud.”

- ***Correction: If the bad actor finds the correct credentials for the application, all encryption melts away.***

“We have back-ups and insurance, so we are not too concerned about cyber attacks.”

- ***Correction: Back-ups are often encrypted or infection at the same time, or immediately after, the primary network is attacked, and insurance coverage does not guarantee a painless, easy, or complete restoration. Sometimes, insurance may only cover minimal costs associated with the event. It is entirely dependent on the type of coverage.***



# COMMON MISCONCEPTIONS

“If it did happen, we just wouldn’t tell anyone.”



2024-08-04	<a href="#">Ma****ny</a>	<a href="#">ragroup</a>
2024-08-04	<a href="#">Ranney School</a>	<a href="#">rhysida</a>
2024-08-03	<a href="#">hlbpr.com</a>	<a href="#">ransomhub</a>
2024-08-03	<a href="#">nursing.com</a>	<a href="#">ransomexx</a>
2024-08-03	<a href="#">LRN</a>	<a href="#">hunters</a>
2024-08-03	<a href="https://aikenhousing.org/">https://aikenhousing.org/</a>	<a href="#">blacksuit</a>
2024-08-02	<a href="#">Khandelwal Laboratories Pvt</a>	<a href="#">hunters</a>
2024-08-02	<a href="#">Jangho Group</a>	<a href="#">hunters</a>
2024-08-02	<a href="#">Keystone Engineering</a>	<a href="#">spacebears</a>
2024-08-02	<a href="#">Kemlon Products &amp; Development Co Inc</a>	<a href="#">spacebears</a>
2024-08-02	<a href="#">www.normandydiesel.fr</a>	<a href="#">ransomhub</a>
2024-08-02	<a href="#">www.bahia-principe.com</a>	<a href="#">ransomhub</a>
2024-08-02	<a href="#">retaildata11c.com</a>	<a href="#">ransomhub</a>
2024-08-02	<a href="#">q-cells.de</a>	<a href="#">abyss</a>
2024-08-02	<a href="#">Veren Inc and Crescent Point Energy</a>	<a href="#">ransomhouse</a>
2024-08-02	<a href="https://www.valleybulkinc.com">https://www.valleybulkinc.com</a>	<a href="#">cicada3301</a>
2024-08-02	<a href="#">ENEA Italy</a>	<a href="#">hunters</a>
2024-08-01	<a href="#">warrendale-wagyu.co.uk</a>	<a href="#">darkvault</a>
2024-08-01	<a href="#">text/html; charset=utf-8</a>	<a href="#">ransomhub</a>
2024-08-01	<a href="#">mcdowallaffleck.com.au</a>	<a href="#">ransomhub</a>

## CORRECTION:

Websites like Ransomwatch.telemetry.ltd are updated hundred of times per day, searchable, and provide links direct the criminal websites housing the stolen data.

# THREAT ACTOR MOTIVATIONS

- **Ease**
- **Financial Motivations**
  - “Insider trading”
  - Terrorism
- **Disruption**
  - Hacktivism
  - Political Motivations
- **Zero-Trust**
  - Ability to back-door into another system (Federal agencies, larger networks, corporate systems) and escalate access.
  - Bad actors use easiest point of access to escalate to higher-value targets.
- **Fresh Batches of Unscathed Credit Reports (Schools / Custodial Accounts / 529s)**
  - Students often have unfrozen credit – easily accessible and rarely check their credit reports for unauthorized activity.

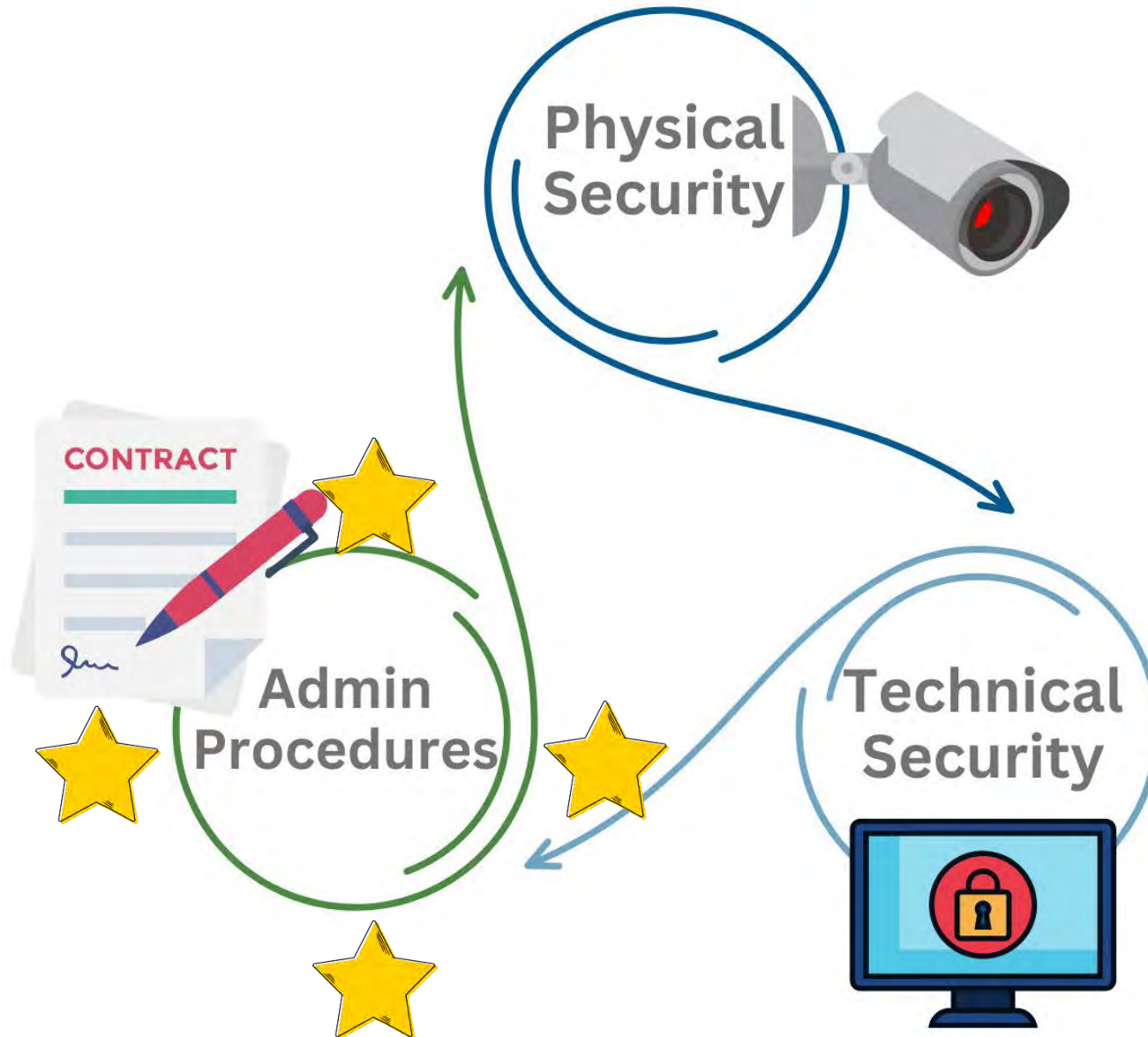






# ADMINISTRATIVE RISK MITIGATION

# TRINITY OF CYBER RISK MITIGATION



Based off healthcare laws, this tri-prong approach is commonly accepted as a complete cybersecurity approach.



# ADMINISTRATIVE POLICY GOALS

## THREE PURPOSES

1. Stop employees from creating or increasing existing cyber vulnerabilities.
2. Alert you to employee errors or intentionally malicious actions.
3. Adhere to regulated data requirements.



**United States  
Attorney's Office**  
Eastern District of New York

PRESS RELEASE

## Brooklyn Woman Pleads Guilty to Unauthorized Intrusion into Credit Union's Computer System

According to court filings, Barile was fired from her position as a part-time employee with the Credit Union on May 19, 2021. Two days later, on May 21, 2021, Barile remotely accessed the Credit Union's file server and deleted more than 20,000 files and almost 3,500 directories, totaling approximately 21.3 gigabytes of data. The deleted data included files related to mortgage loan applications and the Credit Union's anti-ransomware protection software. Barile also opened confidential files. After she accessed the computer server without authorization and destroyed files, Barile sent text messages to a friend explaining that "I deleted their shared network documents," referring to the Credit Union's share drive. To date, the Credit Union has spent approximately \$10,000 in remediating Barile's unauthorized intrusion and destruction of data.



# MANDATORY ADMINISTRATIVE POLICIES



- **Anti-BYOD**  
No “Bring your device policy”
- **Access Policies**  
Who can access which data? *A 20 y.o. receptionist does not need unlimited file access.*
- **Termination Notification Procedures**  
IT/MSSP needs immediate notice of quitting, retired, or terminated employees.
- **Cyber Incident Response Policy**  
PR, Legal, and Tech strategies.
- ★ **Security Awareness Training Policy**  
Helps deter or prevent social engineering.
- ★ **Network Security /Acceptable Use**  
Tells employees the “do’s” and “don’ts”
- ★ **Third-Party Risk Management**  
Vendors (and employees) are HUGE risk factor.



# SECURITY AWARENESS TRAINING

Employees are a company's biggest asset and vulnerability in cybersecurity. An employee can notice early indicators of a cyber incident, allowing the employer to avoid incidents. Alternatively, an employee can inadvertently welcome cyber crime.

## **Recommended** Employee Training:

1. Social Engineering (phishing)
2. Artificial Intelligence Safety
3. Device Safety
4. Identifying Fraud
5. Cybersecurity 101

Most courses are available for free, online, and even through Microsoft licenses for enterprises.

Benefits of these courses may include reduced insurance premiums and protect the business.

## SPAM EMAIL

### SPOT THE DIFFERENCE

there are 6 differences between the fake and real one, can you spot them?

FAKE	REAL
<p><b>From:</b> <a href="mailto:support@microsoft.co.uk">support@microsoft.co.uk</a> <b>Sent:</b> 16/01/2023 11:44 <b>To:</b> Bob Smith &lt;Bob.Smith@company.com&gt; <b>Subject:</b> Urgent Action Needed!</p>	<p><b>From:</b> <a href="mailto:support@microsoft.co.uk">support@microsoft.co.uk</a> <b>Sent:</b> 16/01/2023 11:44 <b>To:</b> Bob Smith &lt;Bob.Smith@company.com&gt; <b>Subject:</b> Unusual Sign In Activity</p>
<p>Microsoft Account</p> <p><a href="#">Verify your account</a></p> <p>We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.</p> <p>To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.</p> <p><a href="http://account.live.com/ResetPassword.aspx">http://account.live.com/ResetPassword.aspx</a></p> <p>Thanks, The Microsoft Team</p>	<p>Microsoft Account</p> <p><a href="#">Verify your account</a></p> <p>We detected some unusual activity about a recent sign in for your Microsoft account <a href="mailto:bo*****@company.com">bo*****@company.com</a>. you might be signing in from a new location app or device.</p> <p>To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.</p> <p><a href="#">Review recent activity</a></p> <p>Thanks, The Microsoft Team</p>

# SECURITY AWARENESS TRAINING



## Identify the Target

Someone with power & authority



## Phish the Target

Study them for likes/dislikes



## Impersonate & Steal Via Email

Redirect revenue and hide the evidence



## The 2023 Las Vegas Cyber Attacks

- Cyber-attack performed by a group known as Scattered Spider, which specializes in social engineering. The attackers manipulate victims into performing certain actions by impersonating people or organizations the victim has a relationship with.
- The hackers are said to be especially good at “vishing,” or gaining access to systems through a convincing phone call rather than phishing, which is done through an email.
- With MGM, the hackers found an employee’s information on LinkedIn and impersonated them in a call to MGM’s IT help desk to obtain credentials to access and infect the systems.



# NETWORK SECURITY/ACCEPTABLE USE

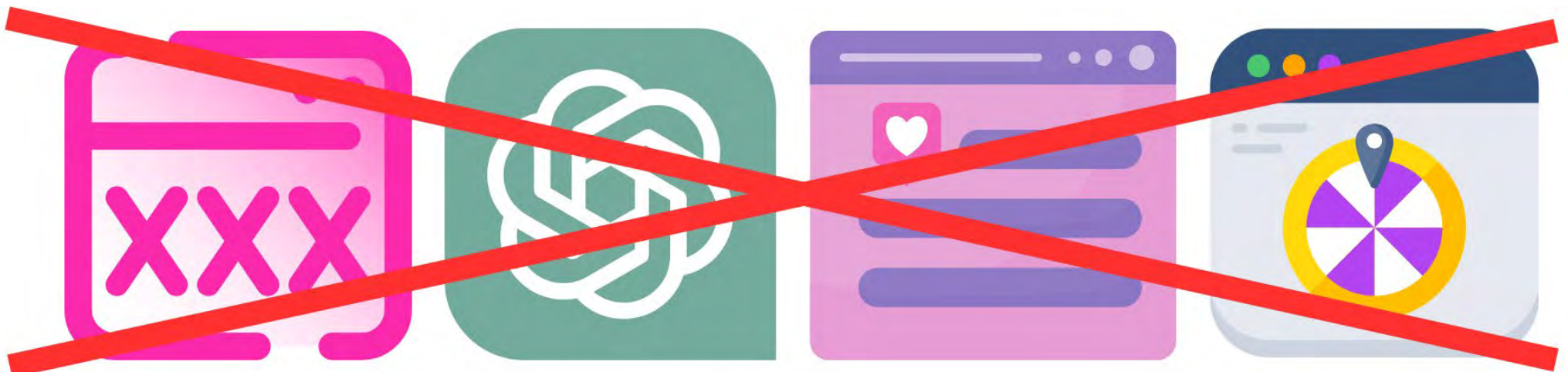
## APPROPRIATE INTERNET USAGE

(examples)

- Only utilize your company issued email platform and address for company business – no diverting to private email addresses.
- Refrain from visiting or accessing any internet sites that are not reasonably related to your duties or position.
- Refrain from posting about workplace activities or plans on the internet absent express written permission from a supervisor.
- Comply with all employer efforts and instructions to back-up user and entity data and implement security measures.
- Timely report any abnormal activities or suspicious emails to the designated point(s) of contact.

## Such Policy, should (at a minimum) include:

- Advise employees that there is “no expectation of privacy.”
- Password policy
- Prohibited Conduct
- Reporting & preventing Lost/Stolen Devices
- Annual Employee Cybersecurity Training
- Reporting Abnormal Computer Activity
- Appropriate Internet Usage





# THIRD-PARTY RISK MANAGEMENT

If you trust a vendor with:

- Employee, customer, or company data
- Network or device access

**THEY POSE A CYBERSECURITY RISK!**

A perfectly sound network is meaningless if a vendor can open the back door for threat actors without your knowledge. A vendor's cybersecurity flaws become **YOUR RISK.**

 **Progress<sup>®</sup> MOVEit<sup>®</sup>**

MOVEit breach: over 1,000 organizations and 60 million individuals affected



**COLORADO**

Department of Health Care  
Policy & Financing







# THIRD-PARTY RISK MANAGEMENT

## INVESTIGATE

Three basic ways to evaluate any vendor providing services to your business:

1. Google Search the Vendor – use keywords like “cyber attack” or “lawsuit” next to the Vendor’s name and see what pops-up.
2. Require vendor to complete a cybersecurity questionnaire – many are free and open source.
3. Ask your attorney to search legal databases for lawsuits involving vendor, as well as any liens or bankruptcy filings.
4. Set up Google alerts on vendors.
5. Request proof of third-party cyber insurance coverage.
6. If they claim patented tech, ask for patent number.
7. Request AI use info and (ideally) prohibit it.

## RESTRICT

Principle of least privilege



Utilize the principle of “Least Privilege” and implement a policy requiring vendors to use on-site vetted devices can help mitigate the risk associated with unsecure devices.



# THIRD-PARTY RISK MANAGEMENT

## CONTRACT

(Minimum Contractual Provisions)

Vendor relationships are governed by the contract and a good contract reduces risks of expensive disputes by clearly outlining obligations of each party. Each vendor contract needs to include the following provisions:

- Electronic Payment Fraud Mitigation
- Minimum Insurance Standards
- Sublicensing
- Notification Obligations
- Prohibition against Data Utilization
- Cybersecurity Safeguards
- Password Policies
- Pricing & Autorenewals
- Data Retention and Destruction
- Transitions





# COMPLIANCE REQUIREMENTS



# REGULATED DATA



## Educational Data:

- Family Educational Rights and Privacy Act protects the privacy of student educational records. Applies to all schools that receive U.S. Department of Education funds. **No private COA.**

## Data Affecting Minors:

- Children's Online Privacy Protection Act requires websites and apps for kids < 13 to disclose the info it collects, how it's used, and get parental consent. Penalties: \$41K+ per violation. **No private COA.**

## Health Data:

- HIPAA, HITECH, 21<sup>st</sup> Century Cures Act and Interoperability Rules. **No private COA.**
- Genetic data – separate state laws.

## Financial Data:

- Gramm Leach Bliley Act requires minimum "Safeguards" for any institution that performs financial services. Includes hospitals if they offer long-term payment options. **No private COA.**

## Biometric Data:

- Prohibits the collection/distribution of biometric information absent signed consent. Illinois, Texas, Washington, Arkansas, New York, and California have punitive laws.

## Consumer Privacy Laws:

- California, Texas, Washington, Montana, Tennessee, Indiana, Iowa, Florida, Colorado, Connecticut, Oregon, Delaware, Utah, Virginia (20 states) all have consumer privacy laws. Washington State has Consumer Health Data Act.



# NEW A.I. STATE LAWS



- **Illinois:** Currently prohibits use of AI when videotaping job applicants without their knowledge.
- **Colorado:** Colorado SB205 (Consumer Protections for Artificial Intelligence), requires developers and deployers of AI, to use “reasonable care” to prevent “algorithm discrimination” on consequential decisions.
  - \$20,000 per violation.
- **Utah:** Utah’s Artificial Intelligence Policy Act, Utah SB 149, requires AI transparency and accountability.
  - Individuals who provide services of a “regulated occupation” must prominently disclose when a person is interacting with generative AI, and the company remains responsible for violations caused by its generative AI applications.
  - \$2,500.00 per violation.



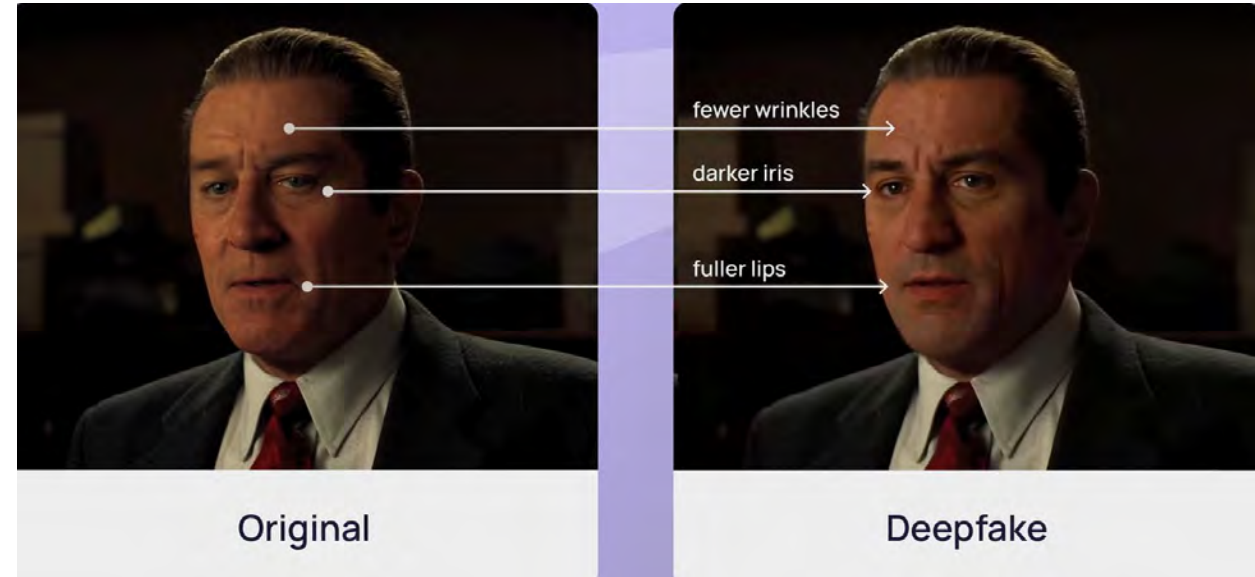


# NEW A.I. STATE LAWS



**California:** 2 new laws effective on January 1, 2026:

- **Assembly Bill 2013: Artificial Intelligence Training Data Transparency Bill**
  - Entities offering use of generative AI systems for CA residents must disclose source/owner of dataset, the number of data points included in the datasets, whether the database was purchased, etc.
- **Senate Bill 942: AI Transparency Act**
  - Applies to entities that offers a generative AI system with over 1,000,000 users/month and is available to CA Residents.
  - Requires entities to offer an A.I. detection tool at no cost that allows a user to assess whether content was created or altered by AI.
  - This bill imposes a civil penalty in the amount of \$5,000 per violation to be collected in a civil action filed by the Attorney General, a city attorney, or a county counsel, as prescribed.





# GLBA SAFEGUARDS RULE

## FINANCIAL DATA (16 C.F.R. §314.2(h))



Effective June 7, 2023, the Gramm-Leach Bliley Act updated/expanded its cybersecurity requirements:

1. Designation of qualified individual to oversee and enforce infosec program.
2. Infosec program to be based on risk assessment against security incident.
3. Design and implements risk safeguards.
4. Regularly test programs and protection.
5. Implement policies and procedures for infosec program.
6. State how you will oversee MSSPs/Infosec providers.
7. Evaluate and adjust information security program following testing and monitoring.
8. ***If have information on 5,000 or more consumers***, establish a CIRP.
9. ***If have information on 5,000 or more consumers***, require its “qualified Individual” to report annually (or more) to controlling body on infosec policy.



# CYBERSECURITY DECEPTION

Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45) prohibits "***unfair or deceptive acts or practices in or affecting commerce.***" The prohibition applies to all persons engaged in commerce.

- “Unfair or deceptive acts or practices” in Section 5(a) includes such acts or practices that cause or are likely to cause reasonably foreseeable injury within the United States or involve material conduct occurring within the United States.
- “Deceptive” practices are defined as involving a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances.
- An act or practice is “unfair” if it “causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition.”



**Office of Public Affairs**  
U.S. Department of Justice

On July 24, 2019, Facebook settled for \$5 billion for violations of its 2012 FTC Settlement and subsequent deceptive trade practices involving its privacy policies.

Newly-issued compliance measures imposed on Facebook included appointment of an independent assessor to monitor Facebook’s conduct, privacy reviews for all new or modified Facebook products, establishment of a new Independent Privacy Committee on Facebook’s Board of Directors, annual compliance certifications by Facebook CEO Mark Zuckerberg, and various reporting and record-keeping requirements. Under the stipulated order, the Department of Justice and FTC will share responsibility for monitoring and enforcing Facebook’s compliance.

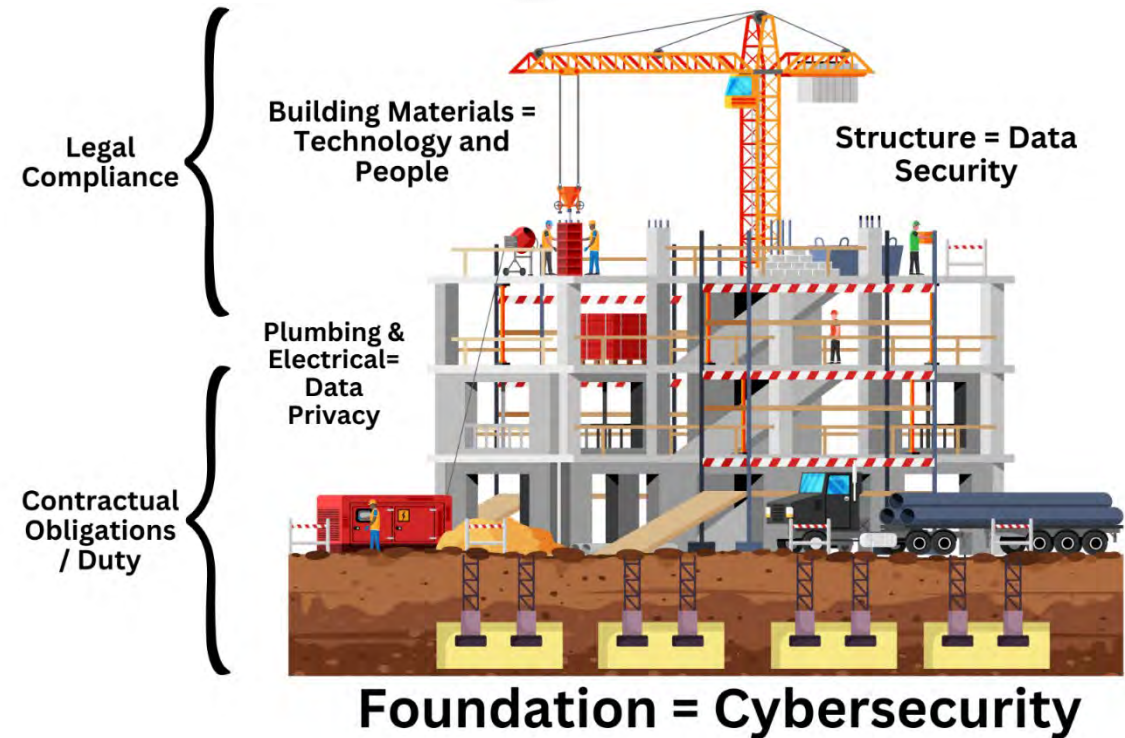




# KEYS TO LEGAL COMPLIANCE

In addition to GLBA...

- Identify regulated data and alert attorney.
- Do NOT over-promise and under-deliver on cybersecurity.
- Implement third-party risk management.
- Block dating websites, ChatGPT/Grammarly, online gambling, and porn websites, TikTok, and RedNote.
- Require consent for EVERYTHING.
- Minimize data collection and avoid biometrics.
- Retain IT Provider (or internal staff) to create a prioritized list of cybersecurity upgrades, with prices for annual review.
- Always HAVE these cybersecurity tools patched and in-use:
  - Firewalls
  - EDR / MDR with SOC agent
  - Secondary Back-up System
  - MFA





# NAVIGATING CYBER INSURANCE COVERAGE

# SHOPPING FOR CYBER INSURANCE

Cyber insurance policies are fully customizable and should be treated as “Cafeteria Style.” The insureds should evaluate the following internal elements before determining the extent and scope of cyber insurance coverage:

- Age of current technology software and hardware.
- Cloud-based or on-premises servers.
- Third-parties with network privileges.
- Number of users.
- Handling of any regulated data:
  - Biometric information
  - Healthcare data
  - Banking information
  - Data belonging to children
- Ability to pay deductibles.
- Engaging in any wiring of funds.
- Cost of downtime (after a cyber incident)
- Potential need to add additional insured(s).



# APPLYING FOR COVERAGE



- Prepare to answer 20+ questions about the network and infrastructure
  - Do **NOT** lie.
- Insurer's questionnaires are intentionally "nitpicky" and the answers are used to feed their analysis tools.
  - Difference between "enforced" and "enabled" MFA.
- If unsure, give the most conservative answer. Better to have a slightly higher premium than have the policy invalidated later for fraudulent disclosures.
  - **BE HONEST, NOT ASPERATIONAL.**
- Questions that begin with "are ***you*** aware" are not asking the employee answering about his/her awareness. The question is asking if the ***entity itself*** (including anyone employed there) has awareness of a particular topic.

Are you aware of a situation or circumstance which could result in a claim against you with regard to issues related to the cyber coverage you are seeking?

Yes  No

a. If yes, please describe:



# SHOPPING FOR CYBER INSURANCE

**BETTERMENT COVERAGE** Older software & hardware; lots of on-premises equipment.

**FRAUD COVERAGE** Lots of employees; engage in several wire transfers.

**THIRD-PARTY COVERAGE** Handling of regulated data; providing essential services for regulated businesses.

**AGGREGATE LIMITS** Lack of governmental immunities for events; large organization; multiple offices.

**LOW DEDUCTIBLE** Do not keep excess cash in operating budget; lots of employees.

**REGULATORY COSTS** Handling regulated data; subject to agency investigations or credit ratings.

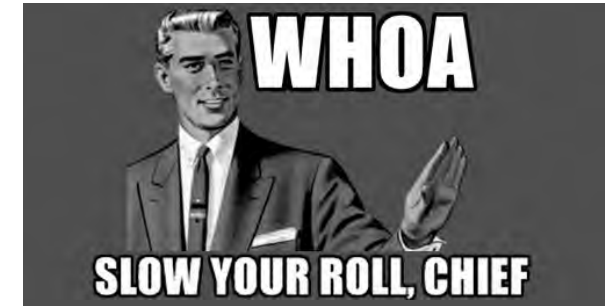
**More employees should =more fraud coverage – watch for MFA reqs. to trigger coverage.**

**Most policies are standardized with first-party coverage for hardware replacement and repairs. Third-party coverage protects the insured from lawsuits, regulatory fines, and claims by entities/persons impacted by the insured's cyber incident.**

# 3 POST-INCIDENT TIPS FOR INSURED



- **DO NOT OVERSHARE** - The insurer will use any info given to them to deny coverage – after giving notice of claim, cooperate but force the insurer to ask questions.
  - Any provision capable of denying coverage will be asserted.
- **YOU DO NOT HAVE TO USE INSURER'S PREFERRED VENDORS** – the insurance company has pre-negotiated rates with cybersecurity vendors. This does NOT mean the vendors are decent, only that they showed the insurer favorable pricing in return for consistent business.
  - *There is a reason people are afraid of "Government Cheese."*
- **MAINTAIN YOUR OWN LEGAL COUNSEL** – breach counsel is an attorney with cybersecurity expertise, pre-selected by the insurer (that YOU pay) to assist with navigating the cyber incident. They represent the insured, but rely on insurer to refer work creating **conflicting loyalties**.
  - Breach counsel have no history with Insured, no motive to maintain that relationship, but a motive to make insurer happy.
  - **Not** always proficient in technology and malware. BUT always looking for quickest band-aid, like paying the ransom.





# EMERGING THREATS

# COOKIE THEFT




**FBI Atlanta**  
Public Affairs Specialist Jenna Sellitto  
(770) 216-3162

 X.com  Facebook  Email

October 30, 2024

## Cybercriminals Are Stealing Cookies to Bypass Multifactor Authentication

The FBI Atlanta Division is warning the public that cybercriminals are gaining access to email accounts by stealing cookies from a victim's computer. A "cookie" is a small piece of data that a website sends to your computer, allowing the website to remember information about your session, such as login details, preferences, or items in your shopping cart. "Remember-Me cookies" are tied specifically to a user's login and often last for 30 days before expiring. This type of cookie helps a user login without having to keep putting in their username, password, or their multifactor authentication (MFA). Typically, this type of cookie is generated when a user clicks the "Remember this device" checkbox when logging in to a website:

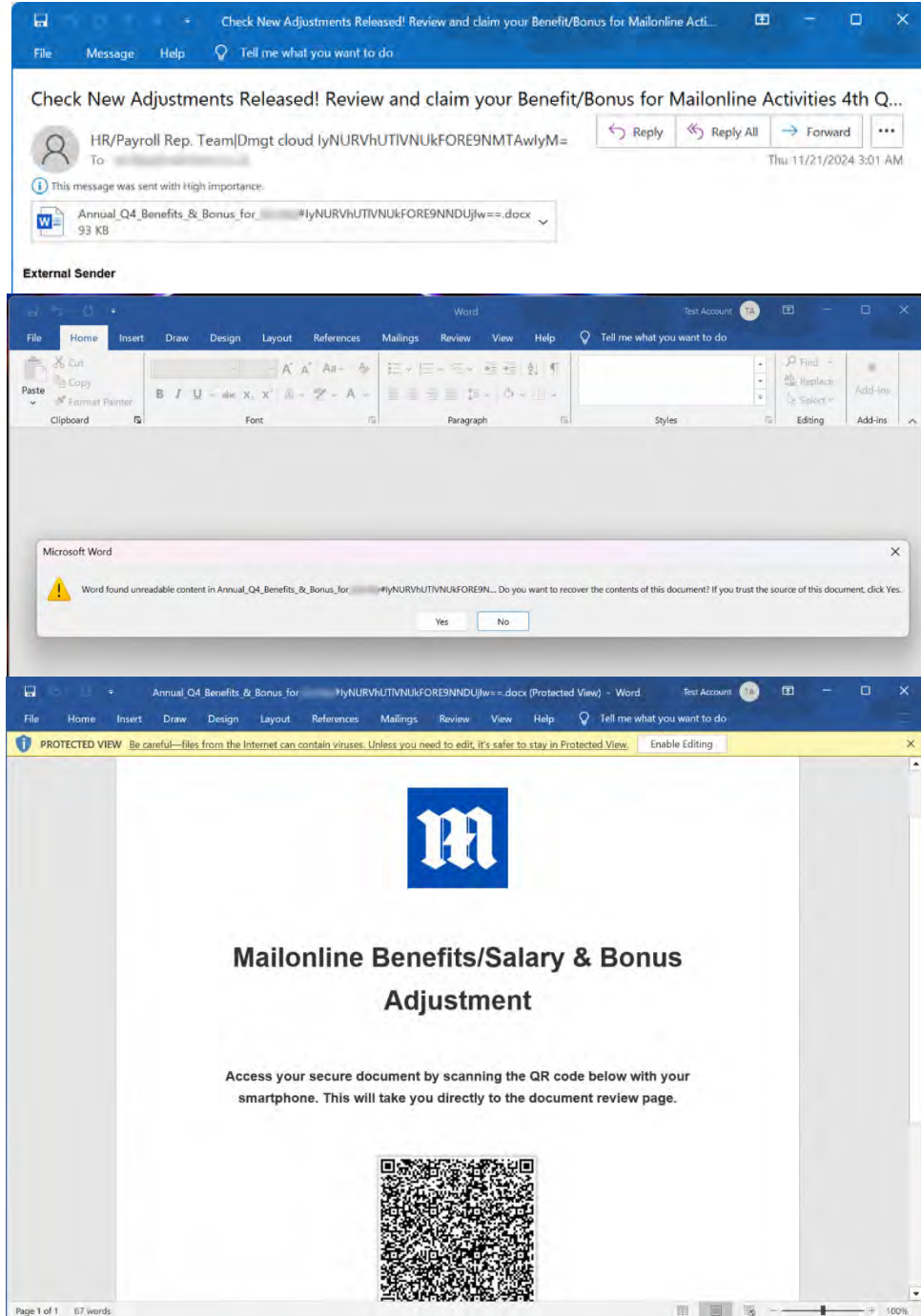


Remember this device for 30 days

Continue

If a cybercriminal obtains the Remember-Me cookie from a user's recent login to their web email, they can use that cookie to sign-in as the user without needing their username, password, or multifactor authentication (MFA). For these reasons, cybercriminals are increasingly focused on stealing Remember-Me cookies and using them as their preferred way of accessing a victim's email. Victims unknowingly provide their cookies to cybercriminals when they visit suspicious websites or click on phishing links that download malicious software onto their computer





# NEW PHISHING ATTACKS

## BLEEPINGCOMPUTER

A novel phishing attack abuses Microsoft's Word file recovery feature by sending corrupted Word documents as email attachments, allowing them to bypass security software due to their damaged state but still be recoverable by the application.

When opening the attachments, Word will detect that the file is corrupted and state that it "found unreadable content" in the file, asking if you wish to recover it. These phishing documents are corrupted in such a way that they are easily recoverable, displaying a document that tells the target to scan a QR code or click a link to retrieve a document. Cyber criminals use real company logos to increase credibility.

Scanning the QR code will bring the user to a phishing site that pretends to be a Microsoft login, attempting to steal the user's credentials or downloads malware.



**SARAH W. ANDERSON**

**OWNER | FOUNDER**

**SWA LAW LLC - LEGALLYCYBER.COM**

**SARAH@LEGALLYCYBER.COM**



**SWA**  
LAW LLC

**2351 ENERGY DRIVE, STE. 1120**

**BATON ROUGE, LOUISIANA 70808**

**OFFICE: 225.256.2892 | FAX: 225.267.8396**