McGriff
A Marsh & McLennan Agency LLC Company

Cyber - The Good, The Bad & The Ugly

troutman pepper locke

Keiter
Your Opportunity Advisors

Disclaimer

This presentation is offered for informational purposes only.

The information in this presentation does not constitute legal or investment advice. Please consult with your legal or investment professional for your individual circumstances.

All McGriff Risk Services' offerings are advisory in nature and are designed to assist the client in the establishment and maintenance of a safe workplace. The responsibility to provide safe and healthful work conditions and operations free from known risk and harm to employees, third parties, and the environment is, and shall remain, that of the client. This proposal, and any subsequent reports, is not a warranty that reliance upon them will prevent accidents and losses or satisfy local, state or federal regulations.

Meet your Moderator

Alan Delahunty

VP, Commercial Lines Agent
McGriff
Alan.Delahunty@MarshMMA.com
Office: 804-938-0056

McGriff
A Marsh & McLennan Agency LLC Company

Meet your Panelists

Chris Moschella, CPA, CISA

Risk Advisory, Senior Manager

Keiter

cmoschella@keitercpa.com

Gene Fishel

Counsel

Troutman Pepper Locke LLP

gene.fishel@troutman.com

Office: 804-697-1263

Agenda

1. Cybersecurity Trends
2. Privacy Law Overview
3. Regulatory Enforcement Actions
4. Regulatory Red Flags

Cybersecurity Trends

Trends, challenges, and takeaways

Cybersecurity Trends

- Supply Chain Attacks
  - Several major supply chain attacks in 2025
- Artificial Intelligence
  - Attacks on models themselves
  - AI used by hackers
  - AI used by defenders
- End users (still) targeted
  - More sophisticated phishing (MFA bypass)
  - More sophisticated ways to infect user devices with malware (ransomware)

Supply Chain Attacks

What is a Supply Chain Attack

A supply chain attack in cybersecurity refers to a tactic where threat actors compromise a trusted third-party vendor, service, software component, or hardware to infiltrate a target organization. Instead of attacking the target directly, attackers exploit vulnerabilities in the supply chain—often the weakest link—to gain access to sensitive systems or data.

Supply chain attacks

15%

of data breaches start with supply chain compromise

Source: *IBM Cost of a Data Breach Report 2025*, pg. 31

Supply chain attacks take the longest to identify and contain

- 196 days to identify
- 71 days to contain

Source: *IBM Cost of a Data Breach Report 2025*, pg. 19

Supply Chain Attacks – Some Famous Ones

2013 - Target Credit Card Breach

~$300 million in losses stem from HVAC vendor

Login credentials stolen from Fazio Mechanical were used by attackers to install data stealing malware on point-of-sale machines.

The malware eventually exfiltrated over 40 million payment cards and personal information of 70 million people.

Total costs, not including impact to stock prices, approached $300 million.

2020 – Solar Winds - Orion

Compromised software update to 18,000 customers

Hackers carried out a sophisticated supply chain attack by compromising updates to SolarWinds' Orion software, an enterprise tool used by thousands of organizations to monitor IT systems.

Automatic updates forced the malicious update to 18,000 customers and provided attackers remote access to victim networks.

In October 2024 – The SEC charged four victim companies with misleading cyber disclosures related to the Solar Winds' Orion attack and agreed to pay civil penalties:

- Unisys - $4 million
- Avaya - $1 million
- Check Point - $995,000
- Mimecast - $990,000

Source: https://www.sec.gov/newsroom/press-releases/2024-174

Supply Chain Attacks – In the News

Clorox sues IT provider

Clorox seeks $380 million in damages from Cognizant

"Cognizant was not duped by any elaborate ploy or sophisticated hacking techniques," according to a copy of the lawsuit reviewed by Reuters. "The cybercriminal just called the Cognizant Service Desk, asked for credentials to access Clorox's network, and Cognizant handed the credentials right over."

The 2023 hack at Clorox caused $380 million in damages, the suit said, about $50 million of which was tied to remedial costs and the rest attributable to Clorox's inability to ship products to retailers in the wake of the hack.

Source: Raphael Satter – Reuters – July 22, 2025

XZ Utils Backdoor

Narrowly avoided a worldwide cyber-disaster

In early 2024, a database developer (accidentally) discovered a malicious backdoor in an open-source Linux data compression tool called XZ Utils, which is deeply integrated into SSH, a system protocol for secure remote system access.

The developer, Andres Freund, was investigating ~0.5 second delay when accessing systems via SSH and eventually found the backdoor.

The backdoor would have allowed hackers to secretly log into millions of infected Linux systems, which powers most of the Internet's server infrastructure.

The infected library was already integrated into development versions of major Linux distributions and was weeks away from being released into Ubuntu 24.04 LTS.

The vulnerability earned a rare **10.0 CRITICAL** severity rating.

The sophistication of this attack suggests nation-state involvement.

Source: CVE-2024-3094

Supply Chain Attacks – In the News

2024 - Polyfill.io

100,000 websites impacted

Polyfill.io provided a widely used service that allowed older browsers to support modern web features.

How Polyfill.io Works
When a user visits a website that used the Polyfill service, a script was automatically downloaded from the Polyfill CDN (cdn.polyfill.io). The script would detect feature gaps between the user's browser and the website's JavaScript code and fill the gaps so the website worked. Very helpful!

February 2024, Funnull, a Chinese company, acquired Polyfill.io and modified the Polyfill code so that it also stole sensitive data and redirected users to scam websites.

Source: https://blog.qualys.com/vulnerabilities-threat-research/2024/06/28/polyfill-io-supply-chain-attack

2025 – Salesloft AI Chatbot Disaster

Third-party Salesforce chatbot causes massive breach

Salesloft provides an AI chatbot called Drift that integrates with Salesforce and allows users to access account information stored in an entity's Salesforce environment.

In 2025 - attackers compromised Salesloft's GitHub source code repositories and from there, they accessed Salesloft's Amazon Web Services (AWS) environment from which they stole OAuth tokens. OAuth tokens are used provide Drift bots access to the companies' Salesforce environments.

The attackers used the OAuth tokens to access the Salesforce environments of 760 organizations including prominent tech giants - like Google, Cloudflare, SentinelOne, Zscaler, and Palo Alto Networks - and steal over 1.5 billion data records.

Source:
https://www.bleepingcomputer.com/news/security/shiny hunters-claims-15-billion-salesforce-records-stolen-in-drift-hacks/

https://securityboulevard.com/2025/09/unc6395-hackers-accessed-systems-via-a-github-account-salesloft-says/

Supply Chain Attacks – In the News

2025 – NPM Mayhem, Part 1

One open-source developer got phished, created chaos

npmjs.com, the largest open-source code repository, is where well-meaning developers from around the world publish their packaged code for free for other developers to use.

Sept 8, 2025 – A single developer, who contributes to several NPM packages that, combined, have over 2.5 billion weekly downloads, was phished and attackers took control of his npmjs.com account.

The attackers surreptitiously published new package versions, that if run in a web browser, could intercept and steal cryptocurrency during transactions.

Direct financial losses were low – but it was a massive wakeup call to web developers.

Source:
https://www.paloaltonetworks.com/blog/cloud-security/npm-supply-chain-attack/

2025 – NPM Mayhem, Part 2

Secret harvesting worm spreads through the NPM registry

Sept 14, 2025 – npmjs.com repositories are targeted again – this time it was self-replicating worm named Shai-Hulud, after the giant sandworms that lived on the desert planet Arrakis in Frank Herbert's Dune universe.

When an infected package was installed, the worm scanned source code for secrets (like GitHub tokens, npm tokens, cloud credentials, etc.) and created GitHub repositories, named Shai-Hulud, that contained the encoded data for the attackers to steal.

278 secrets were reportedly stolen during the attack, and have likely been used to steal data from corporate infrastructure. It is too early to tell the extent of the damage.

Source:
https://www.ox.security/blog/npm-2-0-hack-40-npm-packages-hit-in-major-supply-chain-attack/

https://www.cisa.gov/news-events/alerts/2025/09/23/widespread-supply-chain-compromise-impacting-npm-ecosystem

Supply Chain Attacks

Takeaway

- Robust vendor risk management processes – with documented vendor risk evaluations – are critical, but they are not enough.
- When an organization adopts a new software/cloud tool, it inherits not just that vendor's risk, but the risk of their entire supply chain as well, including their software tools, their software development libraries, their cloud services, their third-party integrations, etc.
  - Risk does not scale linearly with each new vendor; it scales exponentially, and it does so in uncontrollable and unpredictable ways.
  - As organizations integrate more third-party technology vendors – the cumulative likelihood of a supply chain attack asymptotically approaches certainty.
- This reality demands a shift in mindset: In addition to vendor risk management processes, organizations should treat every third-party technology as a potential liability and ask the question "is this tool truly essential to our core business?"

AI-driven attacks

16%

Artificial intelligence enabling more sophisticated attacks

Source: *IBM Cost of a Data Breach Report 2025*, pg. 31

Artificial Intelligence Models are Themselves Being Attacked

- Prompt Injection
- Model Inversion
- Model Evasion
- Data Poisoning

Artificial Intelligence and Cybersecurity

Attackers Use AI to:

- Generate more compelling writing, impersonate people and brands and otherwise generate better social engineering/phishing campaigns
- Write software exploits
- Convert malware to other languages to avoid detection

Defenders use AI to:

- Fill cybersecurity knowledge gaps
- Identify vulnerable software code before it is released
- Assist in threat detection and pattern recognition – analyze huge datasets, including real time data, for anomalies that could be indicative of attacks.
- Perform automated response – varying actions based on perceived risk, e.g., high risk event may instantly sever a device from the network.

End users are still a problem

- The percentage of attacks in which end users are the initial attack vector has dropped a bit – but it is still extremely high.
- MFA bypass attacks on the rise
- New and tricker methods to convince users to install ransomware.
- With AI enabling more sophisticated social engineering/phishing campaigns, end users will see more sophisticated attacks.

Takeaways:

- It is no longer safe to rely on the tell-tale signs of scam emails (or phone calls)
- Users need to be more vigilant than ever
- Training is critical, but it is clearly not enough
- Companies must assume that, eventually, someone *will* fall for an attack. Since you can't predict who or when, the only reasonable defense requires assuming every user computer is hostile at all times and designing networks and systems accordingly.

McGriff
A Marsh & McLennan Agency LLC Company

Target End Users

36%

End users are often the initial attack vector in successful data breaches

Source: *IBM Cost of a Data Breach Report 2025*, pg. 17

Engineering firm wires $25 million to scammers

Scammers used AI 'deepfake' tech to impersonate the CFO in a video call.

> "We can confirm that fake voices and images were used," the company said, declining to give details because the incident was still being investigated. "Our financial stability and business operations were not affected and none of our internal systems were compromised," it said.
>
> After a video conference joined by the company's digitally cloned CFO and other fake company employees, Chan said, the staff member made a total of 15 transfers to five Hong Kong bank accounts before eventually discovering it was a scam upon following up with the group's headquarters.

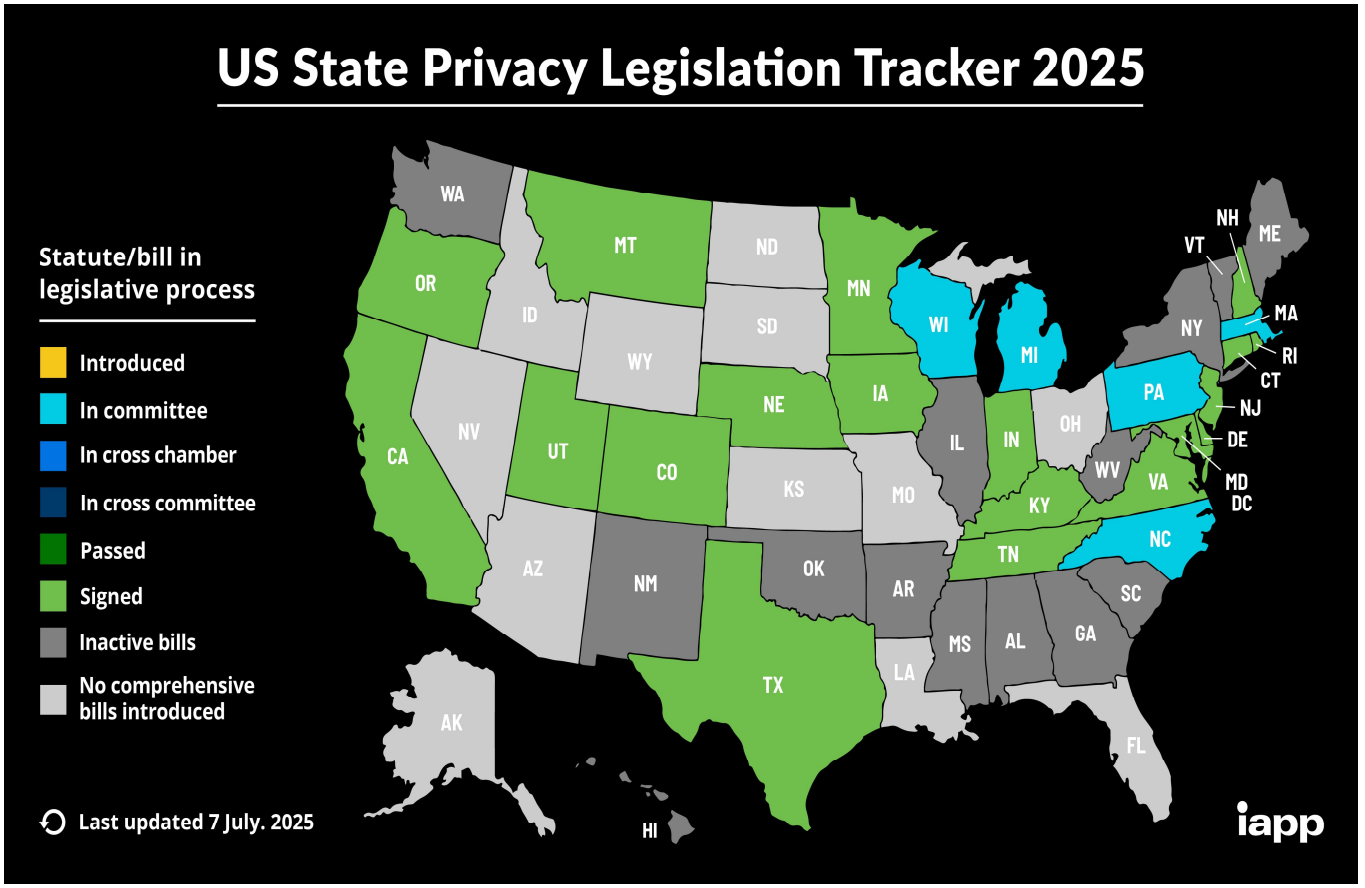
Source: Cheng Leng and Chan Ho-him in Hong Kong – Financial Times – May 16, 2025

Privacy Law Overview

Common elements of comprehensive state privacy laws

US State Privacy Legislation Tracker 2025

- 20 States have enacted comprehensive privacy laws in the last 5 years
- California, Colorado, Connecticut, Maryland, Montana, Oregon, Texas, Utah, and Virginia in effect now
- Most take effect in 2026
- Several others introduced legislation



State Comprehensive Consumer Privacy Laws

Common Elements

Consumer Control

- Notice from controller of data use
- Right to access and confirm
- Right to delete
- Right to obtain a copy
- Right to correct
- Right to opt-out
  - Sale of data
  - Targeted advertising
  - Profiling that produces legal effects

Data Handling

- Limit collection to adequate and relevant data
- Process consistent with notice
- Implement “reasonable” physical, technical, and administrative data security practices
- No processing of “sensitive data” without consent
  - Children’s data
  - Religious beliefs
  - Sexual orientation
  - Mental health info
  - Immigration status
  - Geolocation data

Personal Information—What is it?

- California
  - Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. It includes:
- Identifier such as:
  - Real name, alias, postal address
  - Online identifier, Internet Protocol Address (aka “IP Address”), email address account name
  - Social Security Number, driver’s license number, passport number, etc.
  - Internet activity, including, browsing history, search history, and ad interactions.
  - Geolocation data;
  - Commercial information (e.g., purchase history)…and…

Privacy Related Regulatory Actions

Enforcement

- Virginia Attorney General's Office
  - Consumer Protection Section
  - Computer Crime Section
- VA CDPA Remedies
  - 30-day "cure" period
  - $7500 per violation
  - Injunctive relief
  - No private right of action
- VA Data Breach Notice Remedies
  - $150,000 per violation
  - Potential private right of action
- Limited government resources

Enforcement

- California Privacy Protection Agency
  - Dedicated Privacy Regulator
  - Enforcement Power (including subpoena power)
  - Rule making power
- CA CCPA Remedies
  - No longer mandatory “cure” period
  - $7500 per violation
  - Injunctive relief
  - Limited private right of action--breach following failure to implement reasonable security

Enforcement—Examples

- California Sweeps
  - Online Ads and Sales
  - Opt-outs and Consumer Rights
  - Streaming Services

- California Enforcement Actions
  - Sephora—Settled for $1.2 Million: Failure to provide opt-out of online “sales” related to digital advertising and analytics.
  - Door Dash—Settled for $375K: Failure to provide opt-out of email marketing cooperative
  - Glow—Settled for $250K: Failure to secure fertility tracking app.
  - Various breach settlements (Anthem, Equifax, Kaiser, Aetna, Premera, etc)

Texas AG Enforcement

- Texas AG Ken Paxton announced a lawsuit against an insurance company and its subsidiary under the Texas Data Privacy Security Act (TDPSA) for the allegedly unlawful collection, use, and sale of data regarding the geolocation and movement of Texas drivers
- Also alleged subsidiary violated the state's data broker law when it failed to register with the Texas Secretary of State's Office
- Based on privacy law violations, including failure to obtain proper consent, provide a privacy notice and offer an opt-out method
- The TDPSA's notice requirement for controllers selling sensitive data is a lesson in nuances among state privacy laws

Michigan AG Enforcement

Filed suit against Roku

- Roku fails to protect minor users: The AG asserts that Roku is an "operator" of online services under COPPA, was aware that children use its products, and had specific content directed toward children. Roku allegedly failed to meet its obligations under COPPA by failing to screen for under-age users and obtain parental consent for child users.
- Roku improperly collects, uses, and retains children's personal data: The AG alleges that Roku uses, retains, and sells children's personal data including voice, location, IP addresses, and browsing history in violation of COPPA.
- Roku misrepresents its privacy practices: According to the allegations, Roku's privacy policy failed to disclose its use of the data of minors, which constitutes "unfair, unconscionable, or deceptive" practices that violate consumer protection laws.

Regulatory Red Flags

Aggravating data incident circumstances that may trigger investigations

Regulatory Red Flags

Type of Data Breached

- Greater sensitivity = Greater investigation chance
  - SSNs
  - Health data (diagnoses)
  - Children's data
- Storage method – encrypted v. unencrypted

Numbers and Consumer Demographic

- Higher number = Higher incidence of investigation
- Children's data
- Elderly / vulnerable population data

McGriff
A Marsh & McLennan Agency LLC Company

Regulatory Red Flags

Likelihood of Consumer Harm

- Bad actor v. accidental
- Exposure on dark web

Media Attention

- Public pressure
- Political pressure

Applicable Legal Obligations

- Federal obligations
- State obligations

McGriff
A Marsh & McLennan Agency LLC Company

Regulatory Red Flags

Response of Organization

- Significant delay
- Facially inadequate response
- Obstruction or perceived obstruction
- Law enforcement contact

Regulator Policy Statement Desire

- Higher number = Higher incidence of investigation
- Children's data
- Elderly / vulnerable population data

McGriff
A Marsh & McLennan Agency LLC Company

Questions?

Never settle for less.