An Increasingly Complex Cyber Claims Landscape

2024 Cyber Claims Outlook

April 2024

LOCKTON®

Contents

AUTHOR

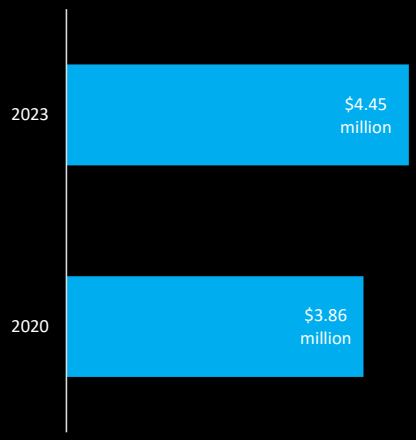
Deb Hirschorn
U.S. Cyber & Technology Claims Leader
816.960.9951
dhirschorn@lockton.com

Over the last decade, cyberattackers have become more sophisticated, regulators have applied greater pressure on organizations to protect critical data and be more transparent about their cyber risk management strategy, and plaintiffs' attorneys have grown more creative and aggressive.

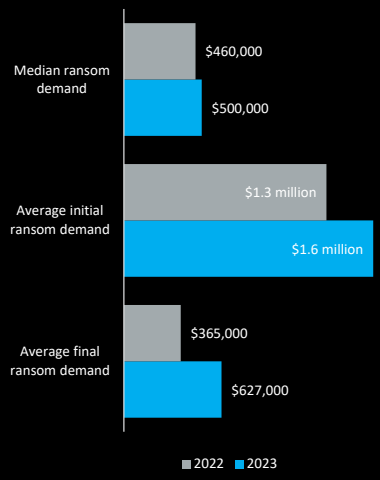
All of this made it more difficult and costly to resolve cyber claims — a trend that will not be reversed in 2024.

Cyber risk at a glance

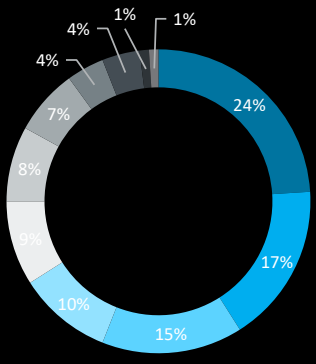
THE AVERAGE COST OF A DATA BREACH REACHED AN ALL-TIME HIGH IN 2023 AND INCREASED MORE THAN 15% FROM 2020.



DEMANDS IN RANSOMWARE ATTACKS AGAINST BUSINESSES CONTINUE TO GROW.

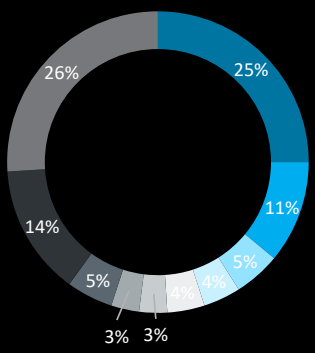


A RANGE OF INDUSTRIES ARE BEING TARGETED IN RANSOMWARE ATTACKS.



- Healthcare
- Finance & insurance
- Business & professional services
- Retail, restaurant & hospitality
- Education
- Manufacturing
- Government
- Technology
- Nonprofit
- Energy
- Other

CYBERATTACKERS USE SEVERAL TECHNIQUES TO PERPETUATE ATTACKS.



- Phishing
- Unpatched vulnerability
- Social engineering
- Misconfiguration
- Employee abuse of access privileges
- Open RDP
- Brute force/credential stuffing
- Other human error
- Other
- Unknown

Sources: IBM, BakerHostetler, Arete

Cyber risk at a glance

Notable cyber events, 2014 to present

APRIL **2014**	Hackers use malware to steal more than 56 million payment card records from a retailer. The breach, which goes undetected for several months, costs the retailer $62 million.
MAY **2017**	"WannaCry" ransomware infects 230,000 computers across 150 countries, causing $4 billion in damage. The ransomware displays ransom notes demanding Bitcoin for a low amount to decrypt files.
JUNE **2017**	NotPetya, a destructive malware, is unleashed on a global scale. Although the main target is Ukraine, NotPetya spreads to 60 countries, destroying computer systems in its wake. Among the most affected organizations is global transport company Maersk, which reports the destruction of end user devices and servers. NotPetya causes an estimated $10 billion in damage.
2017 TO **2019**	Big game hunting, ransomware-as-a-service, and extortionware take off. Focused targets — including major U.S. cities and multibillion-dollar companies — offer cybercriminals increasingly large extortion opportunities and paydays.
2020	Ransomware attacks rise by 150%, according to the Harvard Business Review, amid the COVID-19 pandemic, as remote working presents opportunities for threat actors to take advantage of weak controls. Healthcare is especially vulnerable, and tactics such as double and triple extortion are used by Ryuk and Maze. Data exfiltration becomes essential to double extortion schemes, and phishing emails are a starting point for some ransomware attacks.
2020	Software company Solarwinds and its IT monitoring system, Orion — which provides system management tools for network and infrastructure monitoring for more than 30,000 public and private organizations, including the U.S. government — are targeted in a massive attack. Criminals insert malicious code into the Orion system; when customers update their systems, the code is uploaded into their networks. More than 18,000 customers install updates, with malware spreading undetected.
SINCE MARCH **2022**	Scattered Spider Ransomware Group conducts targeted social engineering campaigns, using phishing pages to capture authentication credentials for Okta, VPNs, or edge devices. MFA codes are then obtained using social engineering or MFA notification fatigue.
MAY **2023**	CL0P Ransomware Group exploits a zero-day vulnerability in a solution software to extort victims and release on the dark web data of those who refuse to pay ransoms.
SEPTEMBER **2023**	Two casinos admit they are victims of Ransomware Group ALPHV/Black Cat, suffering estimated losses of more than $100 million. ALPHV/Black Cat allegedly partners with Scattered Spider to launch a voice-phishing technique to trick IT support and call centers to bypass MFA.
FEBRUARY **2024**	ALPHV/Black Cat targets America's largest healthcare payment platform, causing a massive ripple effect across the U.S. healthcare system.

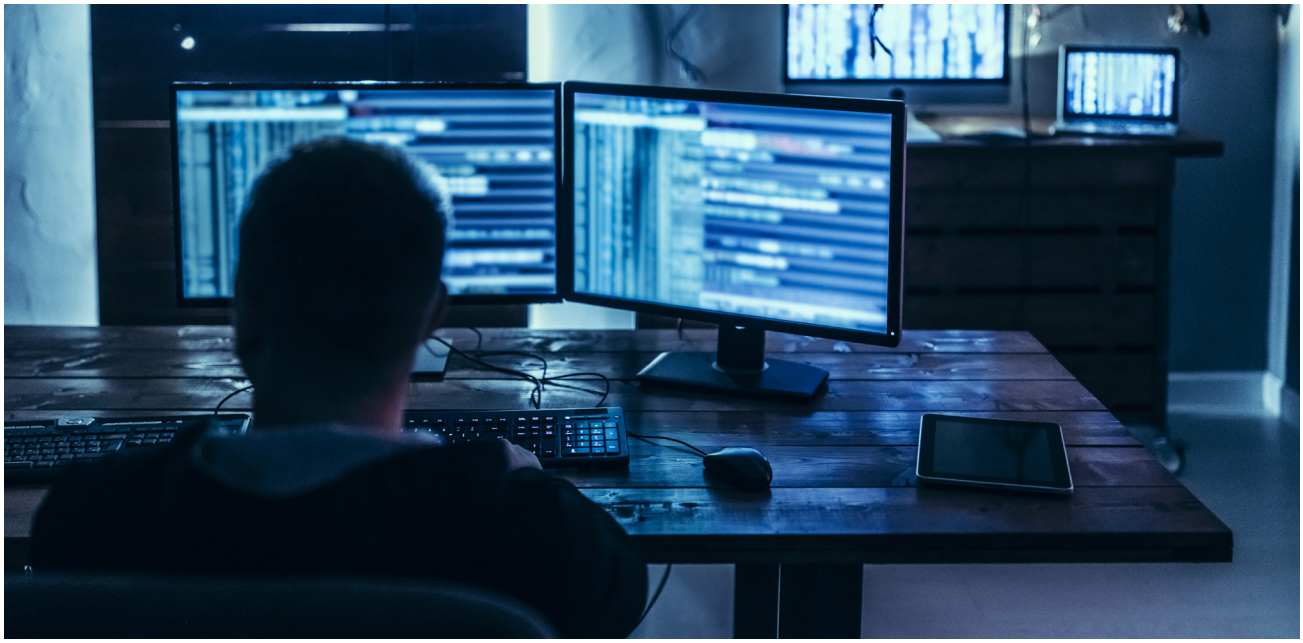
Ransomware threats evolving

In 2024, ransomware remains a significant threat, as attackers demand increasingly large ransoms from businesses, government entities, and nonprofits of all sizes. Further, attack methods are growing more and more complex, moving past basic exfiltration and double extortion and making use of increasingly effective social engineering.

Artificial intelligence (AI) is expected to be the next step in ransomware's evolution. In the past, ransomware attacks carried out via phishing emails could be spotted — by some individuals, at least — owing to the poor spelling and grammar used by perpetrators, who are typically non-native English speakers. But chatbots and other large language model-based tools can help attackers draft emails that appear highly professional, written in perfect English.

Searchable AI databases, meanwhile, can allow attackers to more easily access information on the cybersecurity postures of potential targets, such as which companies have yet to adequately address specific software vulnerabilities. Understanding which companies have such vulnerabilities and which do not enables attackers to engage in "big game hunting" — instead of attacking many organizations in the hope that some will yield results, they can invest time, money, and other resources in targets with confidence that they will produce larger ransoms.

These databases can also enable attackers to look for more than protected health information (PHI) and personally identifiable information (PII). Instead, attackers can go after highly valuable intellectual property.



Privacy litigation a growing concern

> While ransomware clearly remains the primary threat on which most companies are focused, data privacy litigation is quickly moving to the top of cyber insurers' list of concerns.

According to the 2023 Data Security Incident Response Report published by BakerHostetler, a leading privacy defense firm, the number of lawsuits filed after data breaches nearly doubled from 2021 to 2022. BakerHostetler also observed that lawsuits are more frequently being filed over small incidents. "No longer are only the 'big breaches' capturing attention," the law firm said.

Plaintiffs' attorneys are pursuing a number of litigation theories under state and federal laws. For example, under the California Invasion of Privacy Act (CIPA), which took effect in 1967, it is illegal to record confidential conversations without the consent of all involved parties. CIPA provides a private right of action for victims of illegal wiretaps, with the potential for statutory damages of $5,000 per violation.

In recent years, plaintiffs' lawyers have begun to argue that the use of chat boxes — for example, those that pop up saying "Hi! I'm here to help! Please type your question below." — on company websites may violate CIPA. To date, at least 100 class-action suits alleging such violations of CIPA have been filed in California federal and state courts against various businesses, including some prominent national retailers and automakers.

Meanwhile, Illinois' Biometric Information Privacy Act (BIPA), enacted in 2008, introduces specific requirements for companies that use biometric identifiers, including the need to obtain consent to retain and store biometric information. BIPA safeguards the rights of Illinois residents and applies to all private companies that operate in Illinois regardless of where they are based. BIPA's statutory damages are $1,000 for each negligent violation or $5,000 for each intentional or reckless violation.

In October 2022, the first case alleging violations of BIPA — involving a class of 45,600 truckers whose fingers were scanned to gain access to a rail yard — went to trial, with a jury returning an award of $228 million ($5,000 per class member).

The court, however, ordered a new trial as to damages. The parties chose to forego a new trial and settled for $75 million, which provides each class member approximately $1,000. This trial and the Illinois Supreme Court ruling that a BIPA claim accrues each time biometric information is obtained have prompted an increase in the number of BIPA-related lawsuit filings.

Pixel-related litigation continues to develop

A growing concern — particularly for healthcare entities — is online tracking technology, which is used to better understand web users. Such technologies include pixels, small and often invisible images users may unknowingly download when they visit websites, use mobile apps, or open emails. Pixels contain computer code that captures and transmits information about site visitors to the parties placing the pixels, which can include tech companies such as Meta, owner of Facebook, and Alphabet, owner of Google.

Recent news coverage of pixels and allegations that tech companies have used them to collect sensitive health information from visitors to hospital websites have spurred class-action litigation against hospitals and other users of pixels and other tracking tools. The first such suit, filed against a Massachusetts hospital system over the use of pixels without first obtaining consent of website visitors, settled in January 2022 for $18.4 million.

In December 2022, the U.S. Department of Health and Human Services' (HHS) Office of Civil Rights (OCR), which enforces the Health Insurance Portability and Accountability Act (HIPAA), issued a bulletin on the use of third-party cookies, pixels, and other tracking technology by healthcare organizations that largely echoes plaintiffs' concerns. The OCR determined that an individual's IP address qualifies as PHI when the individual visits a regulated entity's website. In July 2023, the Federal Trade Commission (FTC) advised that it will hold companies accountable if they violate consumers' privacy rights by failing to safeguard personal information.

Plaintiffs' attorneys are using often decades-old laws to advance litigation related to pixels. For example, Congress passed the federal Video Protection Privacy Act (VPPA) in 1988 to address the privacy of video rentals after rental company Blockbuster disclosed to the media the video rental history of Supreme Court nominee Robert Bork. In 2012, the VPPA was updated to also cover digital streaming and on-demand services.

Under the VPPA, a video service provider is liable — with certain exceptions — if it discloses a consumer's PII without their written consent. Under the statute, courts may award consumers up to $2,500 in liquidated damages per violation, or actual damages of more, as well as punitive damages, fees, and other equitable relief.

> In the last year, over 115 lawsuits have been filed asserting that pixel tool use violates the VPPA.
>
> These suits allege that pixels track users' activity across third-party websites and send that activity to the companies that placed the pixels to identify the users and target them with advertising.

Lawsuits involving pixels are also alleging violations of federal and state wiretapping laws. Plaintiffs' attorneys have brought class actions against companies that use session replay technology, arguing that using the technology without a consumer's affirmative consent is an illegal wiretap. Plaintiffs' attorneys are relying on a favorable 2022 decision, *Popa v. Harriet Carter Gifts, Inc.,* where the 3rd Circuit U.S. Court of Appeals found that tracking tools intercept communications under state wiretap laws.

Regulators taking action

In July 2023, the Securities and Exchange Commission (SEC) adopted a final rule establishing requirements for incident reporting, cybersecurity risk management, and governance. The rule applies to U.S. public companies as well as foreign private issuers (FPIs). The new rule requires:

- Form 8-K disclosure of "material" cybersecurity incidents within four business days of a company's determination that the incident is material or will result in material changes for investors, and updates without unreasonable delay following discovery. (FPIs are required to disclose this information via Form 6-K.)
- Annual disclosure in Form 10-K regarding the company's cybersecurity risk management and strategy, which should include the company's process for assessing, identifying, and managing material risks from cybersecurity threats. (FPIs are required to disclose this information via Form 20-F.)
- Annual disclosure of a company's cybersecurity governance, describing the roles of the board and oversight processes for cybersecurity risks.

The final rule became effective September 5, 2023 and requires annual disclosure of risk management, strategy and governance procedures, effective for all registrants for fiscal years ending on or after December 15, 2023. The material cyber incident disclosure requirements would be effective on or after December 18, 2023 (smaller companies have a 180-day deferral).

Separately, the New York Department of Financial Services (NYDFS) issued an amendment on Nov. 1, 2023, to its cybersecurity requirements for financial services companies. The amendment introduces:

- New requirements for larger companies (described under the rule as class A companies).
- Expanded governance requirements for boards, senior officers, and chief information security officers.
- Expanded cyber incident notice and compliance certification requirements.
- New requirements for incident response and business continuity planning.
- An expanded multifactor authentication requirement for user access to a company's network.

The amendment requires a covered entity to report a cybersecurity incident to the NYDFS superintendent within 72 hours of determining the incident has occurred. The amendment further clarifies that the reporting obligation is triggered if a cybersecurity incident occurs at a covered entity, its affiliates, or a third-party service provider, and that reports must be submitted electronically via the NYDFS website.

A covered entity is required to provide the NYDFS superintendent with any information requested regarding a cybersecurity incident. Covered entities also must update the NYDFS superintendent of any material changes to the information reported or if new information subsequently becomes available.

Regulated entities must comply with the new requirements by April 29, 2024, although certain provisions allow a longer time frame for compliance. The new requirement regarding reporting certain cybersecurity incidents became effective on Dec. 1, 2023.

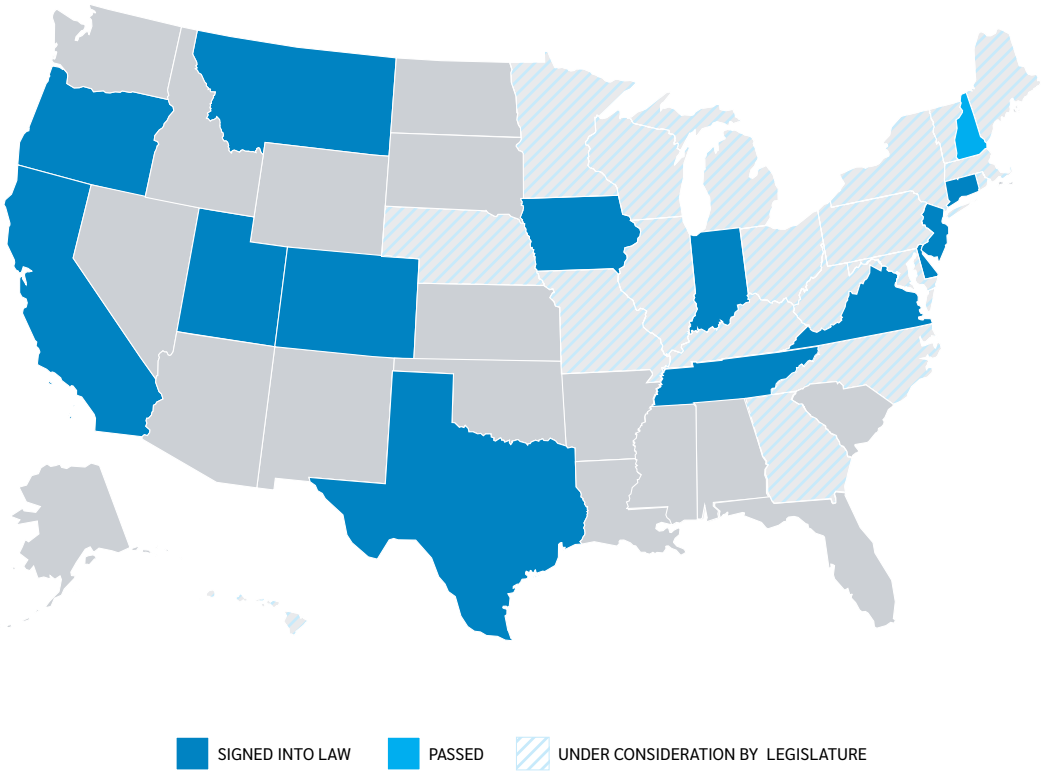
As AI use as reached new heights, state and federal regulators have taken notice. Since 2019, 17 states have enacted more than two dozen bills "regulating the design, development and use of artificial intelligence," according to the Council of State Governments. A major area of focus on several of these bills is data privacy and accountability.

Meanwhile, in 2022, the White House Office of Science and Technology Policy proposed what it called a Blueprint for an AI Bill of Rights, noting that "Unchecked social media data collection has been used to threaten people's opportunities, undermine their privacy, or pervasively track their activity—often without their knowledge or consent." More recently, in February 2024, the Federal Trade Commission proposed new regulation to combat AI-powered impersonation fraud.

State legislation to fuel more litigation

New avenues for consumer litigation are also opening via privacy laws being enacted across the U.S., many of which allow for private rights of action. As of March 1, 2024, comprehensive privacy laws have been signed into law in 13 states, according to the International Association of Privacy Professionals (IAPP), with a law passed in a 14th state — New Hampshire — awaiting the governor's signature (see Figure 1). Legislatures in nearly 20 other states are considering their own privacy laws.

FIGURE 1: NEARLY TWO-THIRDS OF ALL STATES HAVE ENACTED OR ARE CONSIDERING COMPREHENSIVE PRIVACY LEGISLATION.



Source: International Association of Privacy Professionals

As more states finalize their own privacy laws, organizations should be prepared to see the plaintiffs' bar capitalize on them by filing more lawsuits.

Recommendations

As the cyber insurance claims environment grows more complex, organizations can take several steps to mitigate their potential risk. Organizations should consider taking the following actions, among others.

ENACT TECHNICAL CONTROLS TO PREVENT RANSOMWARE ATTACKS AND OTHER CYBER EVENTS. Work with information technology, information security, legal, finance, and operations departments to implement key controls, including:

- Multifactor authentication
- Privileged access management
- Regular backups of key data
- Blocking and filtering
- Endpoint detection and response

FOCUS ON EMPLOYEE AND LEADERSHIP TRAINING. It's vital to build an enterprise culture that recognizes the importance of the human factor in mitigating cyber risks. Establish and promote good cyber hygiene by educating employees not to click on or open questionable links and attachments and conducting periodic testing of workforces' susceptibility to phishing attacks.

INVEST IN INCIDENT RESPONSE PLANNING. Include representation on incident response teams from all departments involved in cyber risk management. Designate a key decision-maker, establish communication protocols, and regularly test plans through tabletop exercises.

UNDERSTAND AND DISCLOSE ANY THIRD-PARTY TRACKING TOOLS USED ON YOUR WEBSITE. Determine what tools are used on your website, prune unnecessary trackers, and make clear which tools are used in your website terms of service.

WORK WITH IN-HOUSE AND OUTSIDE LEGAL ADVISORS TO STAY ABREAST OF EVOLVING REPORTING AND COMPLIANCE OBLIGATIONS. Map obligations required under various laws, with a focus on potential overlaps and inconsistencies.

UNCOMMONLY INDEPENDENT

KC: 3425544