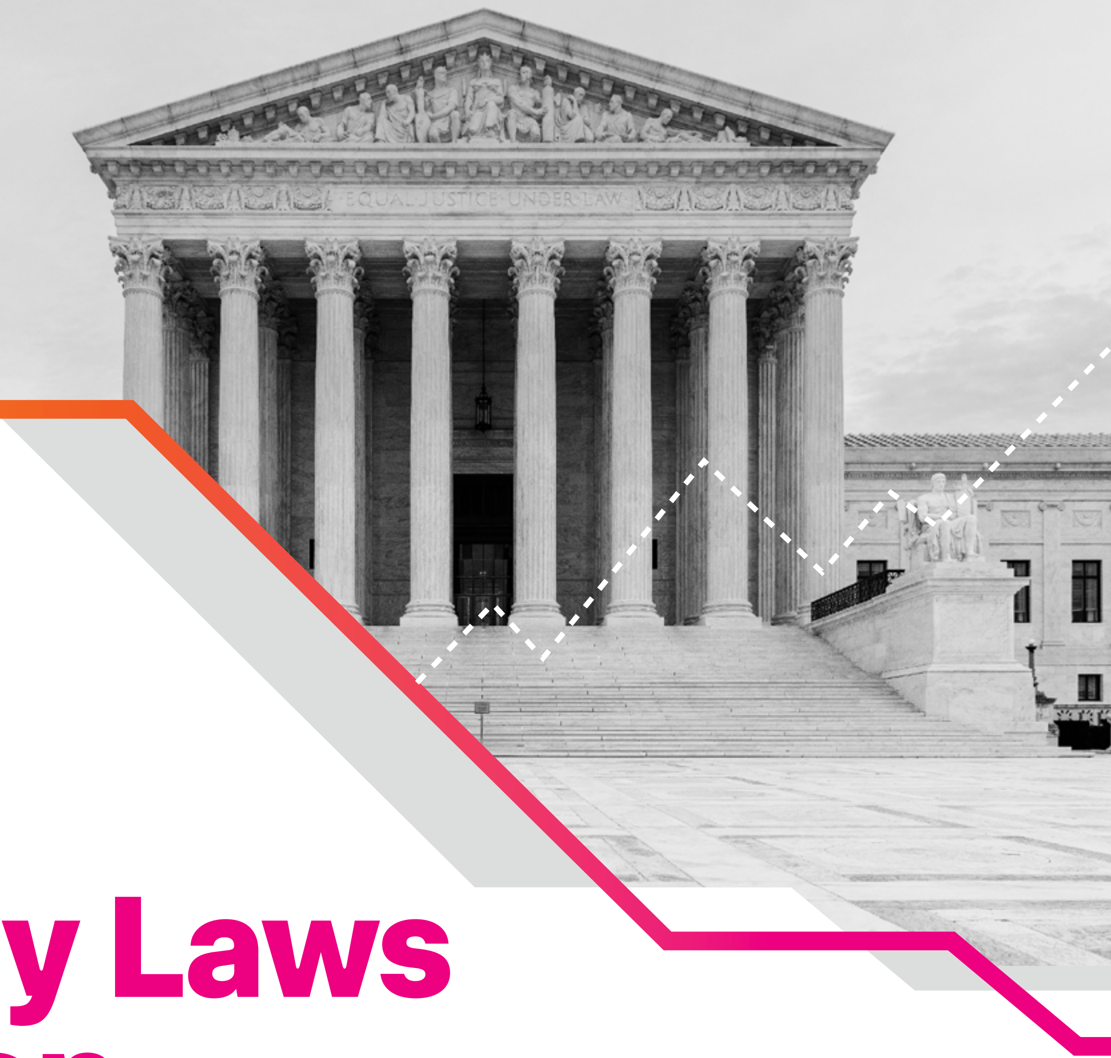


JUNE 2021

Threat Hunter Intelligence Report

Cybersecurity Laws and Regulation

splunk>
turn data into doing™

The Threat Hunter Intelligence Report is a monthly series brought to you by Splunk's threat hunting and intelligence (THI) team. We research and produce actionable reports on the latest cybersecurity threats and trends — helping organizations stay one step ahead of adversaries, one report at a time.

Laws and Regulation 101

May 25, 2021 marked three years since the General Data Protection Regulation (GDPR) was passed in the European Union (EU) — a milestone that raised the bar on data privacy standards, forever changing how we safeguard personal information.

A lot has happened since then. An evolving regulatory environment has changed the very nature of privacy protections, placing even more pressure on chief information security officers (CISOs) to keep customers' data secure, or else face devastating penalties.

In December 2020, the Federal Trade Commission (FTC) and 46 states initiated a pair of antitrust lawsuits aiming to separate Facebook from two of its largest acquisitions, Instagram and Whatsapp. Prosecutors accused the social media giant of weaponizing data and putting "profits ahead of consumers' welfare and privacy," once again placing consumer privacy issues squarely at the heart of a historic regulatory crackdown.

In this month's issue, we explore the shifting attitudes around data privacy, and the influx of regulatory mandates that will inevitably keep CISOs (and their security teams) up at night.

THI profile 1

The General Data Protection Regulation

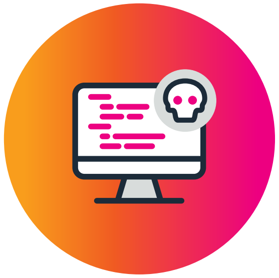
European authorities are enforcing the GDPR in earnest. This means violators — even if well-intentioned — will face serious consequences over the mismanagement of EU citizens' personal and financial information. One example is the 2018 British Airways cyberattack, where half a million customers had their personal information leaked due to the airline's questionable security practices. In response, the UK's Information Commissioner's Office (ICO) lobbed a hefty $26 million fine at the company — and that was *after* reducing the initial penalty.

But somehow, businesses remain undeterred by financial ruin (or something close to it), risking up to €20 million in penalties or 4% of the violator's annual revenue — whichever is higher. A recent study reports that only 28% of companies believe they're fully GDPR-compliant. And GDPR isn't the only mandate that companies need to contend with — the EU's sweeping privacy law paved the way for similar legislation across the pond, including the California Consumer Privacy Act (CCPA), Canada's Consumer Privacy Protection Act (CPPA), and stringent consumer data protections in states like Maine and Nevada.

So, why the lack of consideration for GDPR (and the many privacy acts that followed)? Because these mandates can be difficult to meet — *especially* without the right tools or sufficient resources. Many organizations aren't prepared to deal with so much complexity, and cite significant challenges around legacy IT systems which fail to align to policy, or concerns that a compliance-centric approach would ultimately be cost- and trade-prohibitive.

What you need to know:

To meet the growing demand for data privacy and protection, organizations will need to restructure their security strategy. One approach is to shift to a "privacy by design" model, establishing an information security management system (ISMS) that includes compliance frameworks and policies. There should also be tools for tracking privacy laws and automating compliance tasks, which would help create predictable, repeatable processes — keeping auditors satisfied and eliminating risk.



THI profile 2

U.S. legislation reinforces IoT cybersecurity

Government bodies are looking to standardize security defenses across the Internet of Things (IoT), as well as industrial manufacturing and critical infrastructure. The European Union's NIS directive first laid the groundwork in 2016, establishing risk-based security measures for critical infrastructure and digital service providers (DSPs) in a number of industries, including energy, transportation and healthcare.

Since then, California's IoT Security Law went into full effect — requiring all connected devices to incorporate "reasonable security" measures, namely around user authentication. There's also the IoT Cybersecurity Improvement Act, which looks to the National Institute of Standards and Technology (NIST) to develop mandatory security regulations for all IoT devices used by government agencies. And it doesn't stop there: These provisions apply to consumer devices, including everything from smart TVs and cameras, to virtual assistants like Siri, Alexa, Cortana and Google Assistant.

What you need to know:

These bills take security legislation in a whole new direction, redefining security requirements for a wide range of technologies and — inevitably — informing the future of industrial and consumer markets. Also, a growing interest in this legislative area (ie., IoT cybersecurity) inspires continued scrutiny of connected devices — including what to reasonably expect in terms of privacy and protection, and how best to marry function and security.

THI profile 3

Regulation of artificial intelligence in the U.S. and EU

In the U.S. and EU, strict regulations for artificial intelligence (AI) are being established — meaning widespread consequences should be expected.

In April 2021, the European Commission (EC) presented the Artificial Intelligence Act, calling for better oversight of AI while prohibiting certain use cases and systems. The proposal also includes guardrails around safety and trustworthiness, and looks to the human and ethical implications of AI.

The U.S. soon followed suit, and is building out a comprehensive national AI policy. On January 12, 2021, the National AI Initiative Office became the central hub for AI research and policymaking, with plans to oversee and implement a nation-wide AI strategy.

What you need to know:

Similar to the GDPR, the Artificial Intelligence Act has a number of provisions that could impact companies (and industries) both far and wide. And while the EC's initial draft is likely to change, there's still a chance that the proposal will stay true to form — or become even more stringent.

Regardless of company headquarters, organizations developing or using AI should keep a close eye on the Artificial Intelligence Act (and other policy efforts specific to AI). Depending on the definitions used to determine what use cases are "unacceptable" and "high risk," these mandates could end up applying to a wide range of applications and products, and have a far-reaching effect on innovation.

Violator profile

Cambridge Analytica

Wanted for violating data privacy laws

An infamous violator of data privacy laws is none other than Cambridge Analytica. Defunct since May 2018, Cambridge Analytica was a British consulting firm that exploited the profiles of U.S voters, successfully harvesting the data of up to 87 million Facebook users — the biggest breach in Facebook history.

The plan of attack was simple yet insidious. Unsuspecting Facebook users gave a third-party application permission to access their data, only for the app developer to turn around and give their personal information to Cambridge Analytica, explicitly violating Facebook's terms of service.

When the scandal broke, the outrage was immediate. Lawmakers and regulators, not to mention the public at large, were shaken by the blatant abuse and misuse of users' data and the questionable practices that may have influenced the 2016 election.

Unsurprisingly, there was an urgent call for better safeguards against data exploitation. And not too long after, the GDPR was officially passed, followed by U.S. and Canadian data privacy acts.

Eventually, Cambridge Analytica folded under the immense (and rightful) scrutiny. And in 2019, it was reported that Facebook expected to be fined up to $5 billion by the FTC for privacy violations. Facebook also reported this projected amount in their quarterly financial results.

Violator type:

Private Sector

Suspected country of origin and support:

U.S. and UK

Motivation:

Profit

Go phish

Dark Crystal RAT

The Dark Crystal remote access trojan (RAT) is socialized via email — luring unsuspecting victims into clicking an embedded URL that opens up a document in Microsoft Office. This allows the bad actor to exploit a vulnerability within the software, dropping a payload that's sure to return dividends. But mileage may vary. This threat can be propagated through social media, application downloads or updates and pirated copies of popular software services, in addition to the ever popular, age-old email tactics that most phishing attacks employ.

Developed in Russia, the Dark Crystal RAT was originally available on a website that — to many a hacker's disappointment — was eventually replaced by an irreverent and profane Q&A written in Russian. The hacking tool is still available, however, and can be found easily (if you know where to look).

Hackers interested in the Dark Crystal RAT can download the basic package and choose to invest in additional modules in order to bolster the tool, such as keyloggers and data exfiltration techniques.

The Dark Crystal RAT's long list of capabilities include (but are not limited to):

- Executing remote commands
- Keylogging
- Collecting cookies
- Opening a chat box to communicate with the victim
- Managing the file system
- Operating and recording video via webcam
- Recording audio via the microphone
- Collecting clipboard data
- Initializing a remote-control connection
- Downloading or uploading files from their server to the infected host (and vice versa)
- Opening URLs via the default browser of the user
- Managing active processes
- Compiling and executing C# code

Looking for trouble?

Stay ahead of current and emerging threats by subscribing to our monthly updates on threat hunting and investigation.

Subscribe Now

splunk>®
turn data into doing™