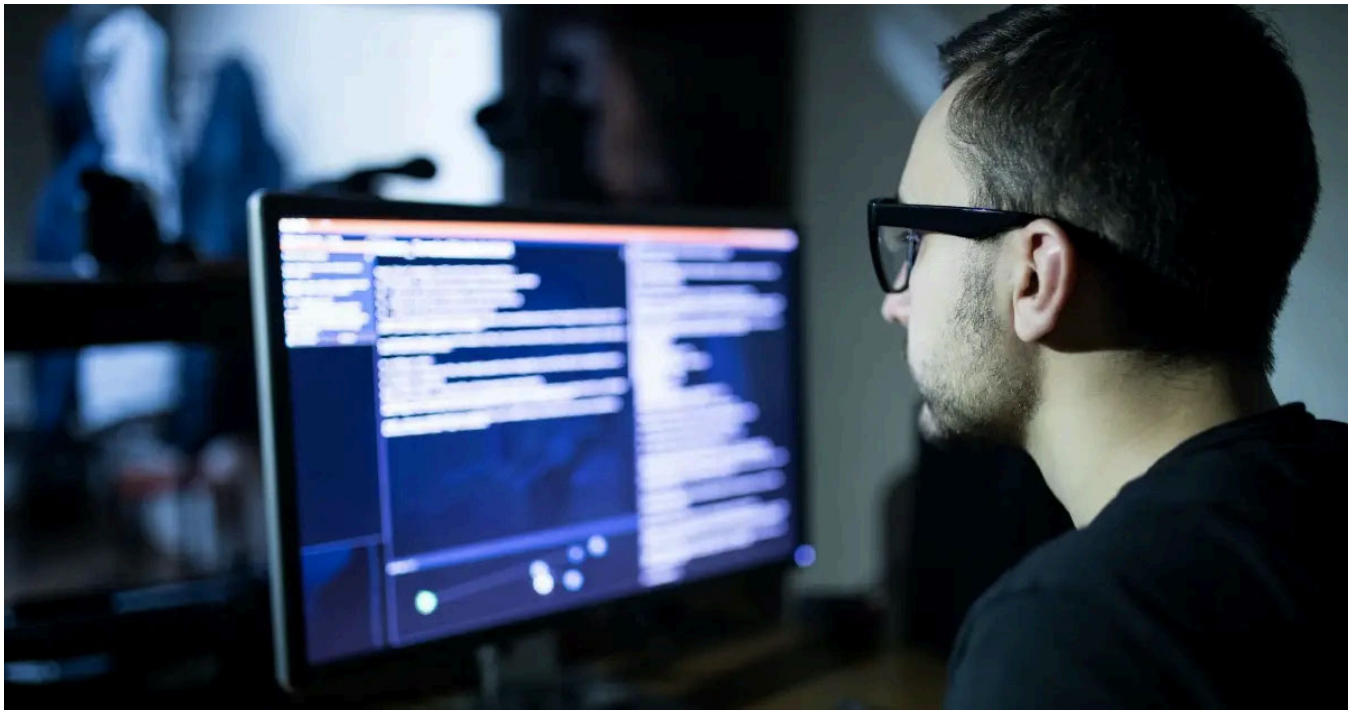
Does a Strong Privacy Program Make for a Stronger Security Program?



Light Dark

February 4, 2021

By George Platsis

4 min read

There is a saying in sociopolitical circles: "politics is downstream from culture." Using that same line of thinking, poses a question: Is information security downstream from data privacy?

In order to tell the difference between *security* and *privacy* and how they feed in to each other to achieve both, we'll look at the leading regulation: the National Institute of Standards and Technology (NIST) Privacy Framework.

Information Security Versus Data Privacy

Why do you secure something? You secure something because you want to keep it private. After all, it's not exactly like we are in the habit of sharing client data, personally identifiable information, intellectual property or the nuclear codes. All of that should be private. In turn, the rightful owner of the data must secure it. And, that is what makes for an interesting discussion about the difference between cybersecurity and privacy.

Cybersecurity and information security measures are often designed around keeping information safe and available, as a whole. On the other hand, privacy measures tend to be more focused on the processing of personal data and privacy rights.

We may be in the middle of a shift. Laws and frameworks centered around privacy are gaining even greater traction. You could make the argument that much of the shift is a result of protecting the privacy of customer data. For example, a 2019 Pew Research study revealed

- Concern about how much data apps collected.
- Concern that people collecting that data are not holding it as securely as it once was.
- People feel their online actions are being tracked.
- Few people know what is being done with the data being collected on them.
- Most people accept, but do not read, privacy policies.
- Most people see more risks than benefits from personal data collection.

National Efforts to Increase Privacy

With this shift in public opinion comes an increased focus on privacy and cybersecurity law and protecting personal data. Some examples just over the last couple of years include:

- The European Union's General Data Protection Regulation (GDPR) from 2018.
- The California Consumer Privacy Act (CCPA), which came into full effect in January 2020.
- More state governments looking at data privacy legislation, in places like New York, Maine, Massachusetts, Nevada, Texas, Washington and even talk of legislation at the federal level.

The federal government is even talking and taking action in regards to American consumer data, notably that mobile app data should be protected and housed within the U.S. due to potential national security concerns. Multiple countries are looking at specific data localization standards in order to protect the data of their citizens and businesses.

It's almost like we are entering into a type of Catch-22 situation, whereas we create and integrate more secure measures, such as

Perhaps the way we avoid that nightmare is to look at what good privacy looks like and then secure that. And a great place to start for how to make a robust privacy program is the NIST Privacy Framework, which was released in early 2020.

Why is the NIST Privacy Framework a Good Example?

The folks over at NIST may have hit another home run after the wildly successful and industry best practice NIST Cybersecurity Framework (NIST CSF). Designed to improve privacy through enterprise risk management, the NIST Privacy Framework works much like the NIST CSF, where the core is made up of functions, categories and subcategories. In fact, there are even some categories and subcategories that are the same as those in the NIST CSF.

Using both these frameworks in tandem makes for a pretty awesome program for both information security and data privacy.

The core functions of the NIST Privacy Framework are:

- **Identify:** Develop the organizational understanding to manage privacy risk for people arising from data processing.
- **Govern:** Develop and implement the organizational governance structure to enable an ongoing understanding of the organization's where privacy risk informs risk management priorities.
- **Control:** Develop and implement plans to enable groups or people to manage data with sufficient detail to manage privacy risks.
- **Communicate:** Develop and implement plans to enable groups and people to have a thorough knowledge and engage in a dialogue about how data are processed and related privacy risks.
- **Protect:** Develop and implement data processing safeguards.

updated (September 2020) NIST Special Publication 800-53rev5, Security and Privacy Controls for Information Systems and Organizations.

Perhaps one of the most helpful tools of the NIST Privacy Framework is the roadmap, which identifies priority areas that describe key challenges and some initial activities.

Why Privacy May Be an Easier Sell than Security

What if we begin to apply that 'privacy mindset' to the business as a whole, not just personal data? That could have a profound impact. After all, in many countries, corporations do have some sort of individual rights. In the U.S., for example, the Supreme Court extended some, not all, protections guaranteed to individuals in the Bill of Rights to corporations.

One of the greatest challenges security experts always face is getting people to 'buy in' to protection. Putting security downstream from privacy may be one way to get the buy in you need, exactly because privacy can be pictured more easily. There's something more emotive and personal about privacy than the more generic 'security' concept. The NIST Privacy Framework addresses issues from that perspective, too. Just a small sample of examples that illustrate that personal nature includes:

- Categories of people (e.g. customers, employees or prospective employees, consumers),
- Context (e.g. demographics and privacy interests or perceptions, data sensitivity and/or types, visibility of data processing to users and third parties),
- Stakeholder privacy preferences,

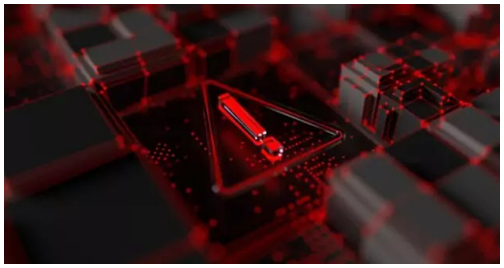
Next to understanding business operations and having the ability to speak knowledgeably on that issue to the decision makers, getting stakeholders to buy in to security through a strong privacy program based on something like the NIST Privacy Framework may be the most important tool in your persuasion arsenal. If ‘security first’ isn’t working for you, try ‘privacy first’ and let security follow.

Data Privacy | Privacy | Privacy Regulations | Security

George Platsis

Senior Director, Educator and Author

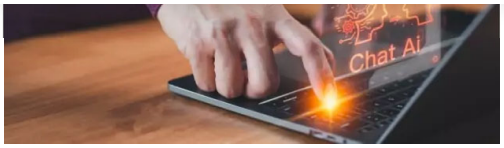
POPULAR



ARTIFICIAL INTELLIGENCE | April 30, 2024

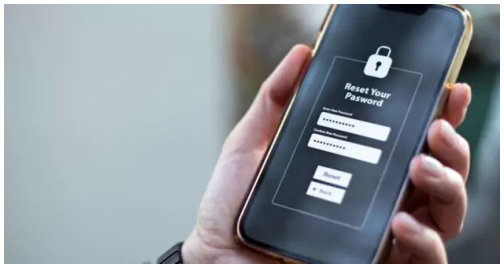
AI cybersecurity solutions detect ransomware in under 60 seconds

2 min read - Worried about ransomware? If so, it’s not surprising. According to the World Economic Forum, for large cyber losses (€1 million+), the number of cases in which data is exfiltrated is increasing, doubling from 40% ...



targeting generative AI systems

2 min read - Researchers have created a new, never-seen-before kind of malware they call the “Morris II” worm, which uses popular AI services to spread itself, infect new systems and steal data. The name references the original...



IDENTITY & ACCESS | April 23, 2024

Passwords, passkeys and familiarity bias

5 min read - As passkey (passwordless authentication) adoption proceeds, misconceptions abound. There appears to be a widespread impression that passkeys may be more convenient and less secure than passwords. The reality is...

MORE FROM DATA PROTECTION

March 27, 2024

3 Strategies to overcome data security challenges in 2024

3 min read - There are over 17 billion internet-connected devices in the world — and experts expect that number will surge to almost 30 billion by 2030.This rapidly growing digital ecosystem...

March 12, 2024

How data residency impacts security and compliance

3 min read - Every piece of your organization's data is stored in a physical location. Even data stored in a cloud environment lives in a physical location on the virtual server. However, the data...

March 5, 2024

From federation to fabric: IAM's evolution

15 min read - In the modern day, we've come to expect that our various applications can share our identity information with one another. Most of our core systems federate seamlessly and bi-...

Topic updates

Get email updates and stay ahead of the latest threats to the security landscape, thought leadership and research.

Subscribe today →

Analysis and insights from hundreds of the brightest minds in the cybersecurity industry to help you prove compliance, grow business and stop threats.