iapp

INFOSEC

A Professional's Guide to Vital Privacy Knowledge

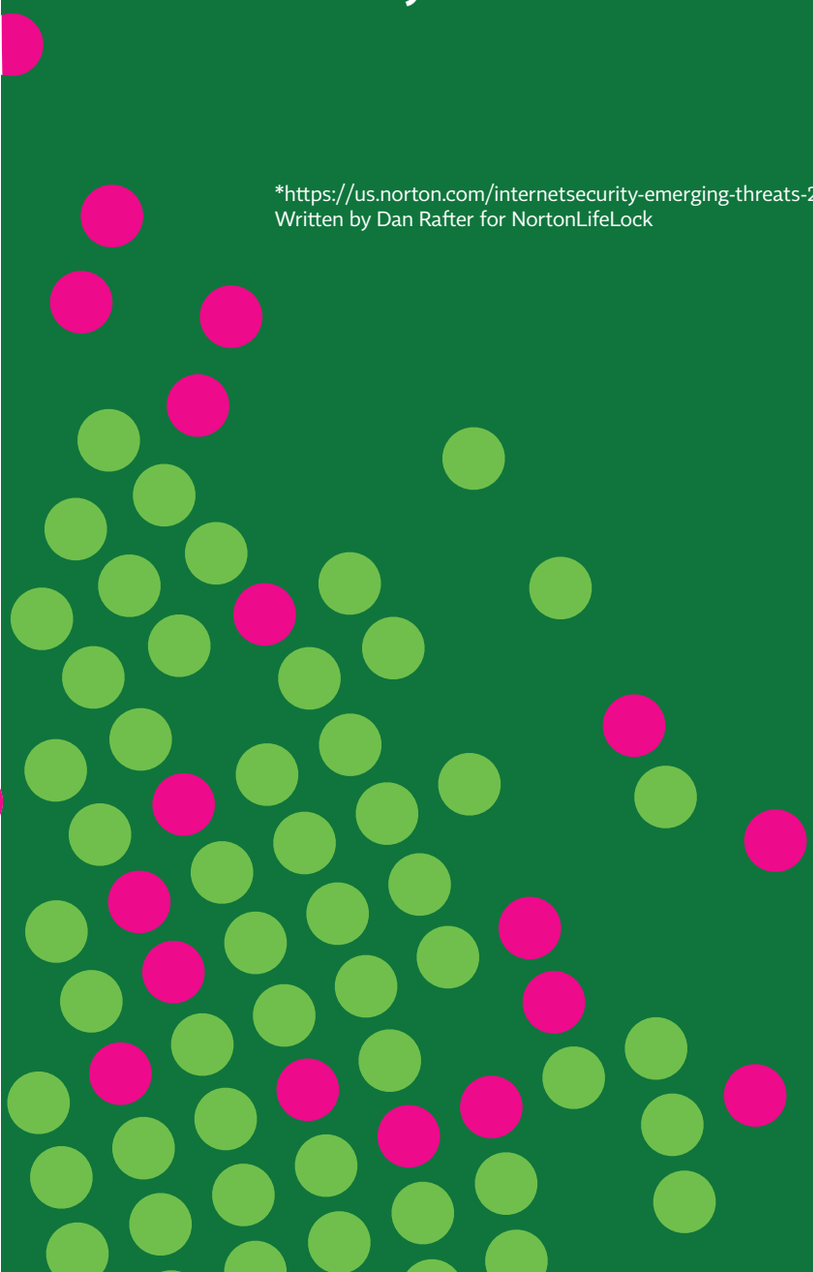
How individuals and teams can acquire the dual literacy they need.

FEATURES
A DETAILED PRIVACY KNOWLEDGE MAP
FOR INFOSEC

As companies continue to sweep up vast amounts of personally identifiable information (PII), data breaches have increased exponentially. In the first six months of 2019, there were over 3,800 publicly disclosed incidents, an increase of 54% over the first half of 2018.*

Consumers are reacting with concern and anger, demanding more control over their data. At the same time, policymakers around the globe are responding with ever-increasing regulations that mandate how this data can be captured, stored and used — and with what degree of transparency. All this means it is more important than ever for infosec professionals to acquire vital dual literacy in privacy and security.

*https://us.norton.com/internetsecurity-emerging-threats-2019-data-breaches.html
Written by Dan Rafter for NortonLifeLock



GAIN PRIVACY KNOWLEDGE OR RISK THE CONSEQUENCES.

"From a business perspective, the reality is that data about us is going to drive everything we do and the way we interact with each other," said Mark Thompson, Global Privacy Advisory Lead at KPMG | United Kingdom. "This creates a whole new kind of security landscape, which is increasingly centered around PII data risk."

To combat this, companies are beginning to look at privacy as a key part of a business strategy that will enable them to leverage data and create business value, while managing the ever-changing liability landscape. "Otherwise, you risk the consequences of heavy penalties and lost consumer trust," Thompson said.

PRIVACY AND SECURITY ARE BECOMING INEXTRICABLY LINKED.

"Traditionally, security professionals have been focused on access control," said Dana Simberkoff, Chief Risk, Privacy, and Information Security Officer at AvePoint Inc., "whereas privacy professionals were more concerned with intent: the purpose, limitation and minimization of information. Potentially, those two things can line up, but not always."

ShanShan Pa, head of U.S. & EMEA compliance at Alibaba Cloud, sees a lessening of the separation between the privacy and security domains. "Technology is growing so fast, that line is getting more blurred every day," she said.

The result is that security and privacy responsibilities within the corporate sphere are beginning to converge. "The whole idea of 'reasonable security' as part of a privacy program means it is now the responsibility of security teams to understand privacy. And that has been a big shift," Simberkoff said. "Privacy laws have significant consequences such as regulatory fines and breach requirements that fall squarely on the shoulders of security. So, there is really no way you can separate the two domains in theory or in practice."

"I think it is a natural evolution for the privacy and security domains to come together," said Alex Grohmann, a certified information privacy technologist (CIPT) with Sicher Consulting LLC and Senior Fellow with the Information Systems Security Association (ISSA). "Security is really about protecting an asset of value. And now we are realizing just how much individual privacy is related to that."

"The goal is protection," said Pa. "Only if security and privacy functions head in the same direction, can we achieve that goal."

> "The whole idea of 'reasonable security' as part of a privacy program means it is now the responsibility of security teams to understand privacy."
>
> ***Dana Simberkoff,***
> *Chief Risk, Privacy, and Information Security Officer at AvePoint Inc.*

MEASURE YOUR PRIVACY INTELLIGENCE.

Use the detailed chart accompanying this white paper to find your title and assess which pieces of privacy knowledge are critical to your specific infosec function.

Managers can use the chart to help set and measure infosec team expectations, goals and skill sets. "I would also use it to build out a comprehensive training program," added Simberkoff.

For individuals, the information can provide a mini-framework of privacy related concepts and help define career growth trajectories. "Adding technical certifications is good, but they are only part of the overall knowledge a security professional must possess," stated Grohmann.

THE INCREASING FOCUS ON PII MAKES DUAL LITERACY EVEN MORE URGENT.

"Security professionals need to stop thinking about privacy as an afterthought or add-on," said Simberkoff. "As a security expert, it is up to you to encourage your colleagues to think about privacy at the whiteboard stage of product development. Companies should be transparent about why they are collecting information, what they need it for, and what they are planning on doing with it. And along with that comes a duty to protect it."

Grohmann agreed. "Infosec people need to look at things through a different lens and realize what may not have been important before, is now. After all, once certain PII is compromised, there is no getting it back. For example, if a social security number is disclosed, the person will not be getting a new one issued, unlike a compromised credit card," he said.

MAKING SURE SECURITY TEAM MEMBERS HAVE THE RIGHT PRIVACY KNOWLEDGE.

The amount of privacy knowledge required by infosec professionals varies by position just as it does with marketing, human resources and other functional areas throughout the enterprise. Yet, as the impact and regulation of PII accelerates, it is difficult to imagine any security function that will not need some degree of privacy knowledge.

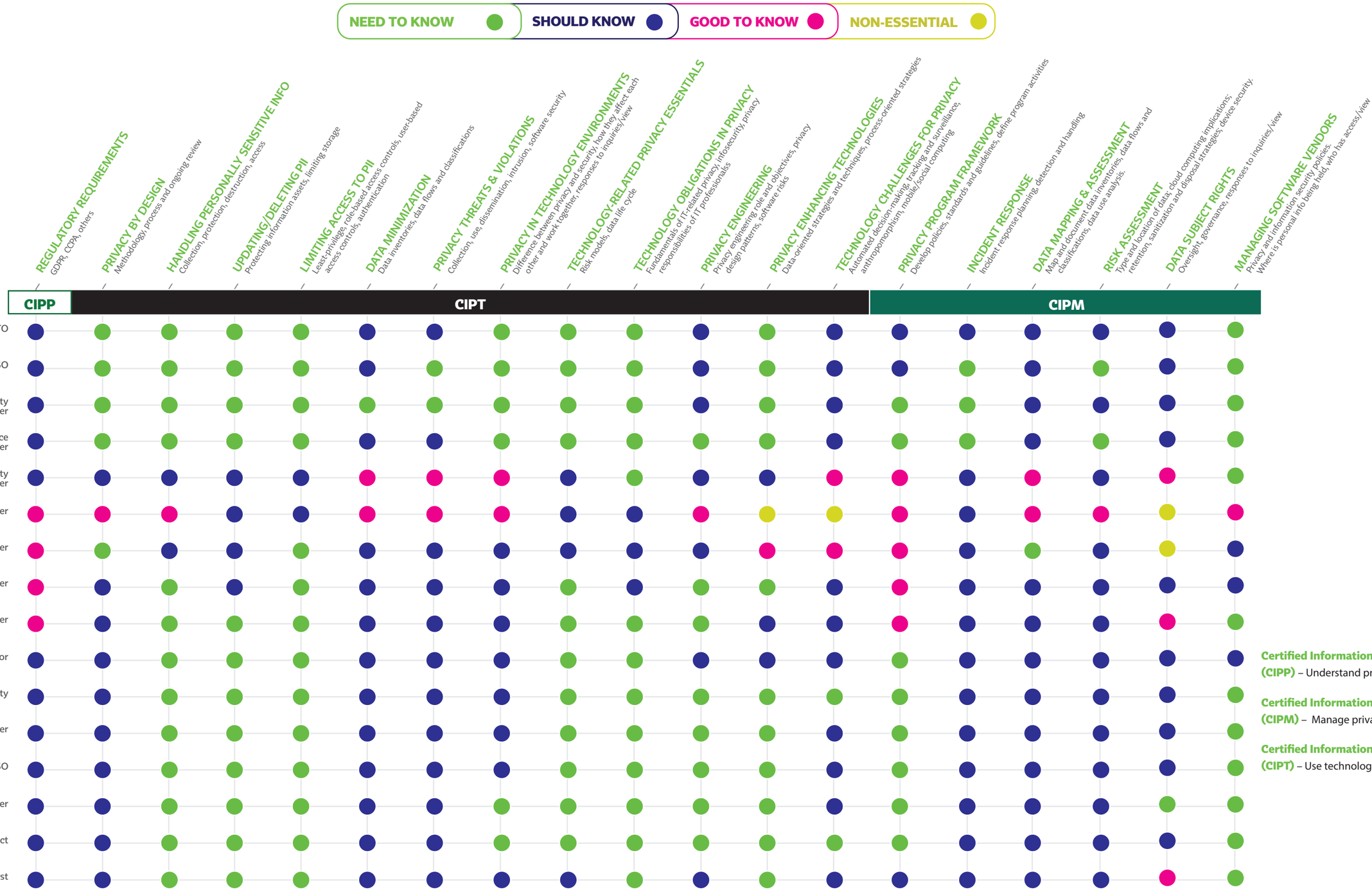
"From a security perspective, you are concerned with making sure that valuable assets and information are secure," said Thompson. "From a privacy perspective, you need to ensure that the collection, use, retention and disclosure of data is in line with consumer expectations, your legal obligations, and your company's policies and procedures. It is critical that the right people understand the risks associated with those assets, and that they know who is actually responsible for owning that risk."

To put this in the proper context, the accompanying chart details the broad spectrum of infosec roles and responsibilities and shows the degree to which deep privacy knowledge is vital for each role. Security professionals can use this to evaluate the current status of their operation, see which areas need improvement, understand the knowledge gaps, and develop an action plan to get themselves and their team up to speed.

> "The goal is protection. Only if security and privacy functions head in the same direction, can we achieve that goal."
>
> ***ShanShan Pa,***
> *head of U.S. & EMEA compliance at Alibaba Cloud*

INFOSEC PROS: BUILD YOUR PRIVACY MUSCLE

Use this grid to assess individual and team privacy skill sets and develop a roadmap for professional development.



Certified Information Privacy Professional (CIPP) – Understand privacy laws and frameworks.

Certified Information Privacy Manager (CIPM) – Manage privacy program operations.

Certified Information Privacy Technologist (CIPT) – Use technology to solve privacy issues.

FLUID PRIVACY LANDSCAPE REQUIRES ONGOING KNOWLEDGE UPGRADES.

"Infosec professionals have to be constantly in the mode of active learning," said Grohmann. That is because gaps in knowledge can lead to penalties or fines for their operations. Ongoing training, conferences, webinars, security blogs, listserves, journal articles and other industry offerings help security people stay up to date on the latest technical security landscape, as well as the ever-changing regulatory environment.

"It is also important to be a part of a community and to build a network of peers — both in your industry and others — to have mentors and provide mentorship," said Simberkoff.

Grohmann agrees. "It is incredibly important to understand the human aspect of obtaining critical and relevant information. You can only read so many things in a textbook and even then the knowledge could be outdated in the current fast-paced world."

As far as certification goes, both Grohmann and Pa believe it is the primary way security professionals can demonstrate they have the requisite privacy knowledge.

"Having a privacy certification is just as important as any of the technical security certifications that you get," said Grohmann. "Probably more so, as you progress in your career and move to more strategic roles, your knowledge must keep pace. It can absolutely set you apart."

Pa concurred, "It definitely helps you get your foot in the door."

> "Privacy knowledge has become a basic staple for the information security professional."
>
> ***Alex Grohmann*** *CIPT,*
> *Sicher Consulting LLC and ISSA Senior Fellow*

PRIVACY KNOWLEDGE COMPLETES YOU AS AN INFOSEC PROFESSIONAL.

"Being fluent in the knowledge of privacy gives you the ability to speak differently or to think about arguments differently than you might without that depth of privacy expertise and vice versa," Simberkoff said. "People with that knowledge are going to be highly sought after." Simberkoff knows of what she speaks. As someone with a background in both law and technology, she is responsible for her company's security and privacy in a joint domain.

Grohmann agreed. "Privacy knowledge has become a basic staple for the information security professional," he said. "The further you move up the ranks, with more areas of responsibility, there are tenets you just need to know. What is next in the emerging privacy space that impacts security professionals? What is new? What are the ramifications of proposed laws and regulations? What do security departments need to do to be ready? Like in chess, one must think three to five moves ahead."

WHY IT IS VITAL TO INCREASE YOUR DEEP PRIVACY KNOWLEDGE NOW.

There is no question that privacy concerns are adding new dimensions to the security landscape and creating new challenges for infosec professionals. The convergence between security and privacy responsibilities within the corporate sphere is happening. By expanding your privacy knowledge base and developing dual literacy now, you can be on the forefront of helping your company or operation leverage data, deliver great customer experiences and create business value while managing business risk and protecting the customer. Within an ever-changing privacy landscape, those are vital skills.

ABOUT THE IAPP:

The International Association of Privacy Professionals comprises the foremost body of resources, knowledge and subject matter expertise dedicated to helping define, promote and improve the data protection profession globally. As a not-for-profit association, the IAPP serves **corporate** and **individual** members operating in diverse functional areas – customer service, finance, human resources, information security, legal, marketing, sales and technology – so they can better navigate today's data-driven world. In addition to providing the only **globally recognized credentialing programs** in information privacy, the IAPP offers practitioners a forum to share best practices, track trends, discuss and debate issues, and provide education and guidance on opportunities in the field.