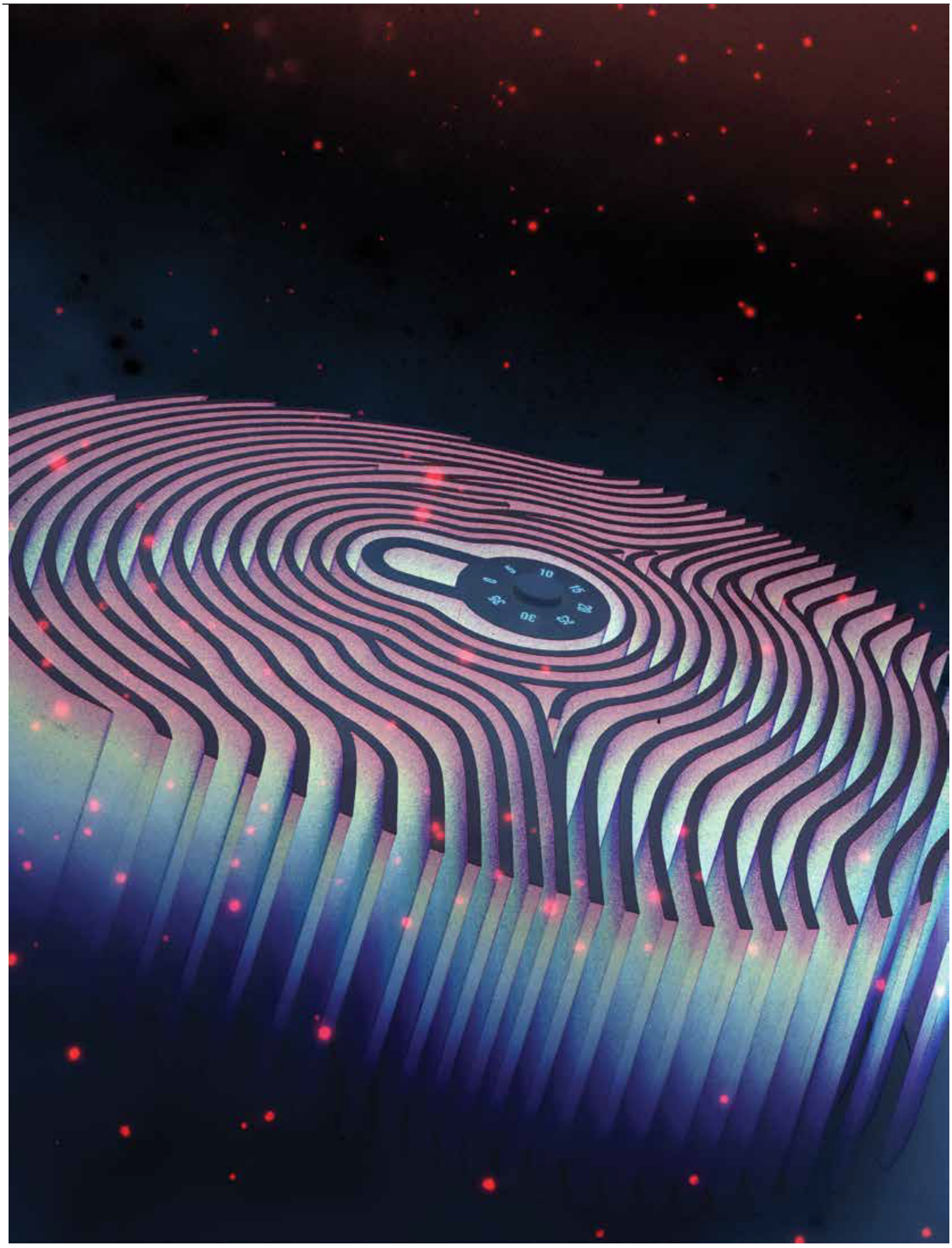
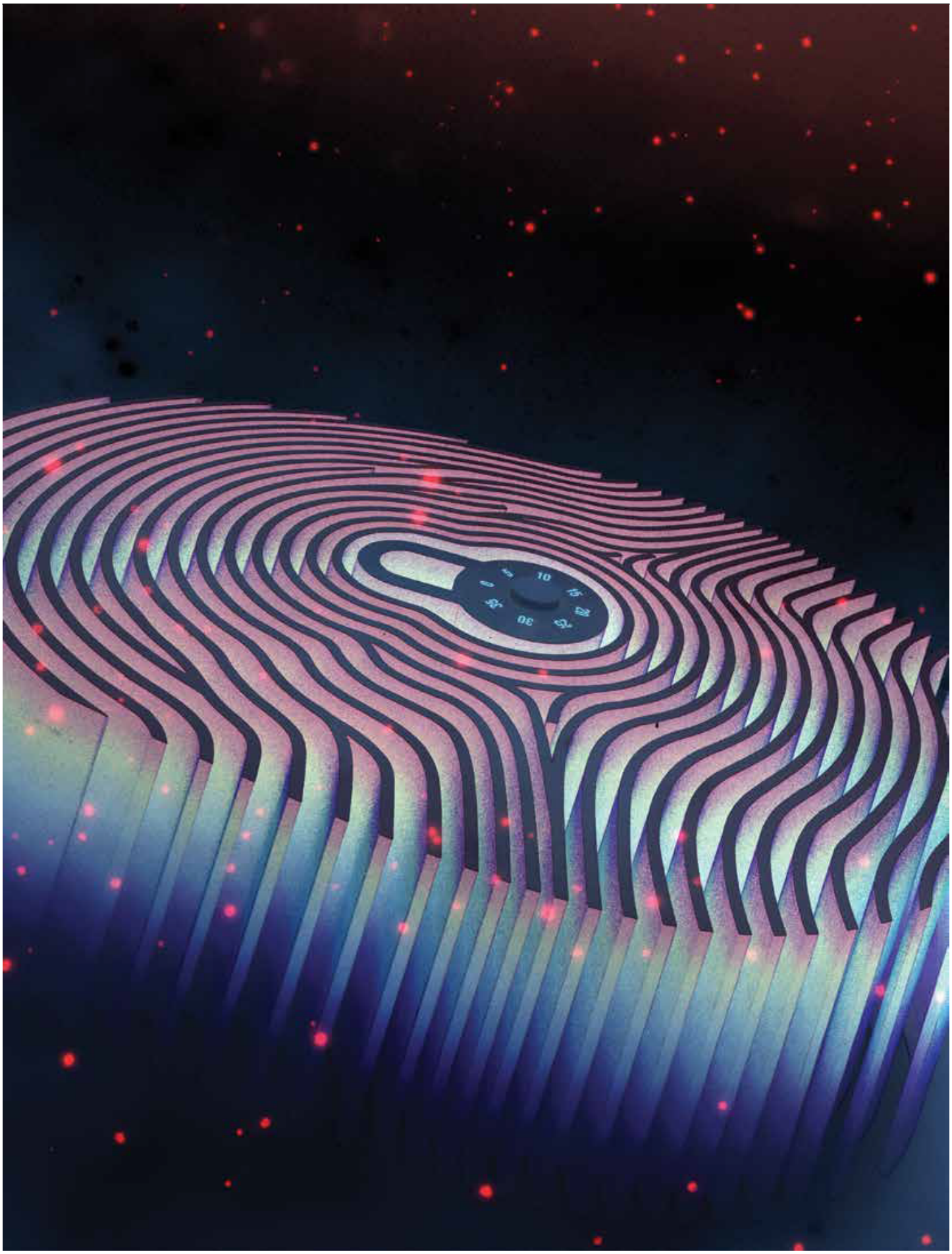
ACC DOCKET
INFORMED. INDISPENSABLE. IN-HOUSE.

The Chief Privacy Officer: The New “Must Have”

Technology, Privacy, and eCommerce


10
15
20
25
30



CHEAT SHEET

- ***Company needs.*** Most companies employ a chief privacy officer to support compliance with privacy and breach regulations, protect corporate data, minimize negative brand impact, and ensure ethical behavior across the organization.
- ***Necessary skillset.*** As the leader of the privacy team, the chief privacy officer must be knowledgeable on privacy and data security laws and be able to communicate effectively with internal and external clients.
- ***Primary responsibilities.*** The chief privacy officer is responsible for the coordination of all functions related to privacy, especially the implementation of a company's privacy policy, assessments, and audits.
- ***Role evolution.*** In the future, the role of the chief privacy officer will most likely merge with the chief information security officer to form the chief security privacy officer.

Whether it is the breach of data privacy and consumer trust by major corporations, or the recent statutory and regulatory developments in Europe, the United States, and Asia, privacy has been a hot topic in the news – and it will continue to be as companies rely on personal data to drive business decisions.

But as companies collect and use more consumer data, it is more important than ever for them to review their data collection practices and policies to ensure it is in compliance with the global frameworks that govern the use, safety, and privacy of this data.

Central to this review and compliance is the role of the chief privacy officer (CPO).

What to look for in a CPO

A CPO must have many different skillsets. A CPO must have knowledge of privacy and data security laws. Depending on the industry and the geographies involved, a CPO must also have knowledge of specialized laws such as the General Data Protection (GDPR), the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act, and other industry-specific laws and regulations.

Further, in order to maximize the role, a CPO should have technical knowledge of how and why information is collected, stored, and used by the company. This includes knowledge of IT systems, data flows, and other relevant technical skills. A CPO must be able to successfully navigate between functions such as audit, IT, the C-suite, and the board. A CPO should also have the ability to speak with customers and clients, as well as other outside entities, with respect to how the company secures data and keeps it private. All of these skillsets are critically important to the ultimate success of a CPO and the company they serve.

It is worth noting that it may be difficult to find all of these skillsets in one person. As such, a CPO must be adept at engaging internal and external subject matter experts, as necessary, to support the CPO role. These cross-functional subject matter experts may include the general counsel, the head

of the IT department, the head of risk management, marketing, audit, human resources, and sales.

The CPO is the leader of the privacy team and would be responsible for the coordination of all functions in the organization with respect to privacy. This complex cross-department functionality is a challenging role and one for a person skilled in navigating the different aspects of the CPO function. In order to be effective, the CPO should also have the authority to make the necessary decisions to accomplish the goals and achieve the objectives of the privacy function.

The evolution of the CPO role

Given the many intersections between privacy and data security, one of the things that we believe will become more prevalent is the role of the chief security privacy officer (CSPO). While most organizations have both a chief information security officer (CISO) and a CPO, many organizations might begin to combine these functions into a single division or person to create greater synergy and effectiveness.

Central to this new CSPO role will be the ability of this person or function to understand the technical aspects of data collection, creation, and usage. The CSPO will also need to understand the human aspects of how this data may be used in manners that influence consumer behavior with emerging technologies, including predictive analytics and artificial intelligence.

Traditionally, data has been looked at from a technical standpoint, whereas privacy has been looked at from a human standpoint.

However, with digital transformation and companies collecting more data on individuals through new technologies and data platforms, including data on how individuals act and think, the technical and the human will begin to merge in ways that we may not yet imagine.

Forward-thinking companies will be at the forefront of navigating the merger of these two distinct functions into one.

While still unusual in its application, we predict that the function of the CSPO will become much more prevalent in the near future.

Why appoint a chief privacy officer?

Given the increased collection, storage, and usage of data on customers and consumers, many companies have hired a CPO to help them understand, protect, and use data to further their business interests as well as to ensure compliance with their legal and regulatory responsibilities.

While there are many reasons to have a chief privacy officer, most companies look to one or more of the following reasons:

- Navigating and complying with complex privacy laws and regulations;
- Ensuring adequate attention to privacy at the leadership level;
- Protecting the privacy and security of corporate data;
- Avoiding data breaches;
- Ensuring compliance with breach notification laws when breaches do occur;
- Avoiding interruptions to business operations;

- Minimizing negative brand impact;
- Evolving compliance programs to new “best practices”; and,
- Supporting ethical behavior across the company.

Data breaches are expensive

Data breaches can cost millions of dollars, if not tens of millions. This does not include the reputation hit to the brand or the loss in a company’s market value.

According to an annual report by the Ponemon Institute published in July, the *2018 Cost of a Data Breach Study* found the average cost per lost or stolen data record is US$148 — up from US$141 in 2017. This was an increase of 4.8 percent over 2017. However, the report noted that if a company had an incident response team, they saved approximately US$14 in response calls per stolen record. **Perhaps alarmingly, the same report indicated that if you had a breach, the likelihood of a recurring material breach over the next two years was 27.9 percent.** This high likelihood further underscores the need for an organization to take the security and privacy of the information it has seriously and further underscores the need for a CPO to help lead this effort.

The Ponemon report also indicates that data breaches were most costly in the United States. This is not surprising given the extent of federal and state laws and regulations that govern a data breach. Over the past 12 months, the average notification cost for organizations in the United States in the event of a data breach was calculated at US$740,000 with post data breach response activities averaging US$1.76 million.

On top of the hard costs associated with responding to a data breach or a breach of privacy, the soft costs can far exceed the former. While hard to calculate and dependent on the industry, the loss of consumer trust and confidence can lead to loss of market share and ultimately potentially to the bankruptcy or insolvency of the corporate entity itself. This is especially dangerous for small and mid-size businesses which may not have the financial staying power of large multinational corporations. Increasingly, this is also an area that state and local governments will need to be aware of as they collect and hold the personal information on their constituents.

In the United States, since there is no national data breach legislation yet enacted, most states have enacted data breach notification laws. Oftentimes, these laws are cumbersome due to the patchwork application by state, and they are also expensive for companies to comply in the event of a data breach. Additionally, we are seeing more boards holding executives responsible for the data breach in addition to a dramatic rise in shareholder lawsuits in such instances. Earlier this year, Yahoo settled their data breach-related securities class action lawsuit for US$80 million. This settlement is one of the first substantial data breach-related shareholder lawsuit recoveries.

Put together, these costs have garnered greater attention and oversight by corporate boards and shareholders leading to an increase in corporate spending for privacy and data security.

A down day is a costly day

Interruptions to business operations are very expensive. Even if the operations of a business are not interrupted entirely, privacy concerns may have a real impact on the ability of a business to sell to consumers as well as a tremendous impact on their overall bottom line. Facebook, Equifax, and Target are all examples of how privacy issues contributed to a negative impact on a company’s

bottom line. The Equifax breach was estimated to cost more than US$430 million as of the end of 2017.

Additionally, privacy issues and data breaches may result in increased regulatory and legal scrutiny for companies, along with legal liability from lawsuits and the tarnishing of the brand. It is worth noting that the US Securities and Exchange Commission now requires public companies to disclose cybersecurity risks and incidents in its filings, as well as its board's role in the oversight of those risks . To the extent that cybersecurity risks are material to the business, the company should inform investors about the nature of the board's role in overseeing management of those risks. Accordingly, it is increasingly important for companies to have someone in the privacy role to ensure that the company is managing and reporting its efforts to ensure the privacy and protection of data, particularly consumer data.

Laws and regulations

Over 100 countries around the world, as well as all 50 US states, have privacy laws with respect to the collection, use, and storage of data.

Additionally, many federal agencies in the United States have industry-specific regulations with respect to the collection and use of personal data. Whether it is the banking industry, healthcare industry, or any other highly regulated sector, the use of personal data is becoming increasingly regulated. **Central to a company's understanding of these laws and regulations, the role of the CPO has become more than a luxury.** Many companies use the role to demonstrate their commitment both to the spirit and requirements of the regulations. It is something that both consumers and regulators view as part of a mature and well-managed privacy program. Today, the role of CPO is a necessity for compliance.

A good example of a new data privacy regulation is the European Union's GDPR, which went into effect on May 25 of this year. This new regulation mandates how businesses can use, collect, and manage the information and data of EU residents (i.e., data subjects) and gives those data subjects more control over how companies use this data. Understanding the GDPR and its requirements is central to the role of the CPO for companies that do business in the European Union and fall under the scope of the regulation. The penalties for non-compliance are steep.

The GDPR mandates that a company have a Data Protection Officer (DPO) if it processes or stores large amounts of special categories of personal data, regularly monitors data subjects on a large scale, or is a public authority. Even if a company does not meet these criteria, guidance from the EU regulators highly encourages the appointment of a non-statutory DPO. Companies that employ a non-statutory DPO are held to the same criteria as companies that mandate a DPO. For many companies, the CPO is the DPO as mandated by the GDPR.

In the United States, some of the more prominent laws that CPOs potentially need to be familiar with are the Federal Trade Commission Act, the Financial Services Modernization Act (commonly known Gramm-Leach-Bliley Act), HIPAA, the Fair Credit Reporting Act, and the Electronic Communication Privacy Act.

Further, many US states have enacted their own laws around data privacy and breach notifications. Examples of this include: the Massachusetts 201 CMR 17, the New York Cybersecurity Regulation, the California Electronic Communications Privacy Act (the California Act), and the new California Consumer Privacy Act of 2018, which has some similarities to the GDPR. As such, a CPO will need

to be aware of and knowledgeable about all of these laws and regulations to ensure compliance and be effective at the state and federal level.

Leadership must lead

Increasingly, corporate leadership has become aware of the importance of privacy and data security. According to the aforementioned Ponemon Institute report, the typical data breach in 2017 cost an average of US$3.8 million, which is up 6.4 percent over the prior year.

As such, corporate leadership, boards of directors, and shareholders have begun to pay attention to the issue of privacy.

This increased attention has manifested itself in the elevation of the office of privacy from a department that often resided in compliance to a standalone function led by someone who may directly report to GCs, CEOs, and audit committees. With this increased visibility, however, comes greater responsibility. The CPO must provide strategic leadership to the organization in the areas of privacy and data security.

Further, the CPO must have the support of senior leadership in the company, as well as the entire board. Without this support, the CPO will have a difficult time effectively addressing the requirements of the role.

Ensuring compliance

While the CPO has many responsibilities, perhaps central to the success of the CPO is the oversight of the compliance function with respect to the use of corporate data.

First and foremost, the CPO is responsible for and should oversee the adoption and implementation of a company's privacy policy. This policy details how information is collected, shared, and used across the organization. Also central to the role of the CPO is ensuring that such information is properly secured by partnering with the information security function.

Additionally, a CPO is often responsible for privacy assessments and audits. CPOs should conduct an initial assessment of a company's privacy practices as well as what information the company collects, why it is collected, and how long it is stored. This assessment should detail who has access to the information and what they're doing with it, as well as how and where the information is stored. Where information resides may be very important as different countries have varying requirements for how their citizen's data may be handled, transferred, or stored.

Once an assessment is done, periodic audits of the privacy policy and the corporation's use of the data should be conducted. It is an industry accepted standard that this privacy audit is conducted annually as the information a company collects and how it may be used will likely change. This audit should be seen as an ongoing responsibility of the CPO and not just a one-time occurrence. The CPO must ensure that the corporate entity has policies and procedures with respect to data, and just as importantly, is following them.

The continued role of lawyers in ensuring privacy

Traditionally, if a company did not have a CPO, compliance and privacy fell under the purview of the

legal department. With the rise of the CPO, some companies have separated direct leadership and responsibility of legal and privacy to create a greater focus on privacy.

However, we have found that companies generally have better results when the legal group remains an active and integral part of the privacy function. Additionally, we have often seen the role of the CPO being filled by someone with direct links to the legal department, as the need to interface with lawyers that have the training and regulatory background in changing privacy laws increases. Additionally, lawyers may better assist with navigating corporate and board structures, which is integral to the success of the CPO.

The bottom line

The misuse of personal data will lead to legal and regulatory issues, as well as damage to a company's brand by destroying consumer and shareholder confidence. The resulting loss of market share and valuation can lead to shareholder lawsuits and well as to the dismissal of corporate executives. Due to the evolving complexities and realities of why and how we collect, store, and use data, CPOs have moved from being a luxury to a necessity for most companies.

Securities and Exchange Commission 17 CFR Parts 229 and 249.

George B. Hanna

CLO

SecureWorks

He is responsible for managing all global legal and compliance activities. Before this, he was

executive VP, chief legal and administrative officer for YP Holdings, a large US digital media company. Hanna also served as chief legal counsel for Wellmark Blue Cross Blue Shield, and VP and deputy GC for BellSouth. He earned a Bachelor of Business Administration with a major in finance from the University of Miami, and his JD from the University of Miami School of Law.

Roy E. Hadley, Jr.

Attorney

Adams and Reese (Atlanta)

He serves as independent counsel to companies, governments, and boards on cyber matters, helping them mitigate legal risks and exposures to protect themselves and those they serve. He has previously served in the corporate roles of GC and chief privacy officer, as well as special counsel to the president of the American Bar Association, and special assistant attorney general for the state of Georgia.