Cybersecurity and Privacy Compliance: The Delicate Balance

For companies to be successful in the digital age, they must walk the fine line between cybersecurity and personal information protection for both employees and customers. In this handbook, learn how organizations are striving to balance corporate and personal information protection.
With Personal Privacy—and Safety—a Priority, Where Does It Leave Cybersecurity?

**Data protection. Online** privacy. Public safety. Cybersecurity. All these terms have become huge, intertwined issues in the post Edward Snowden era, as companies struggle to balance maintaining privacy priorities with adequate cybersecurity protection. Information has become a huge business asset for companies in the digital age, and it has come at a price: Data detailing customers’ personally identifiable information and business operations has become a prime target for hackers. With online data security now a corporate priority, businesses have been forced to invest seemingly endless amounts of resources to protect trade secrets, intellectual property and any vulnerable customer data.

The complications come when data security initiatives infringe on personal information protection measures, especially with personal privacy now a top concern for consumer advocates. The U.S. federal government, for example, raised numerous privacy protection questions as it developed legislation to encourage public/private sector information sharing in an effort to improve nationwide cybersecurity. And as privacy has become a priority for consumers, law enforcement says protection measures such as end-to-end encryption work too well and hinder surveillance efforts.

For companies to be successful in the digital age, they must avoid the notion that cybersecurity and privacy are mutually exclusive. In this handbook, we’ll look at how both the public and private sector are struggling to find the right balance between corporate and personal information protection, and discuss strategies you can use to reach this goal.

**Ben Cole**

Editor, SearchCompliance
To Protect Both Data and PII, Build Privacy Into Information Security Processes

**Information is the** heart of most security programs: By design, many of today’s security technologies capture vast amounts of user, system and application data to provide a holistic view of your organization’s vulnerabilities.

Privacy and security should be designed to support each other, but oftentimes these “big data” security platforms create situations where the two practices conflict. To help ensure privacy and data security coexist, carefully choose the practices and technologies to implement in your organization.

When navigating privacy and security interests, it is very helpful—and important—to engage your legal team. Not only can general counsel assist with identifying where privacy and security mandates apply, but they can also arbitrate if and when one concept takes precedence over the other. In particular, international regulations such as the European Union data privacy laws can appear to clash with standard security principles such as user activity monitoring. In those cases, your legal team can provide guidance as to whether personal or employee privacy rights take precedence over the need to protect the organization through monitoring actions.

This can also extend to customer, or “external user,” information as well. In cases where you support Web-based services or applications for customers, the privacy policy may stipulate that you do not collect browsing or other session information. But to adequately monitor for unauthorized activity, companies may find that they do, in fact, need to collect session information.

Legal counsel can be extremely valuable in helping determine the responsibility that the organization has in identifying security issues and/or providing evidence to address litigation matters.
CONFIGURE PRIVACY-READY SECURITY TECH

When it comes to technologies, it’s important to consider that many of today’s security tools such as SIEM, data loss prevention and even proxy servers are designed to capture as much user, system and application information as possible for monitoring and analysis. Configure these tools properly according to your legal team’s opinion regarding user privacy rights can also help maintain a high level of security.

For example, under the EU data privacy laws it would appear that the user activity captured by proxy servers, a very common security platform, conflicts with privacy rights. However, global security specifications such as PCI-DSS are very explicit regarding user and transaction-level logging. In many cases, it depends on your counsel’s legal interpretation as to which type of litigation they are more concerned about defending: claims involving compromised security or complaints from employees about privacy rights violations.

One of the common techniques to avoid privacy concerns when configuring proxies is to simply record system information instead of user login information. Many of the protections that a proxy/content filtering solution offers are still effective, even without logging the authenticated user name. Also, many HR and legal teams can still act on system-level data such as workstation IP addresses should a user visit inappropriate sites or otherwise violate browsing policy.

Similar to proxies, discussions should be conducted with your organization’s HR and legal teams to determine whether user-identifiable information should be recorded at all. But if they determine that this data absolutely needs to be recorded, another option is to mask any personally identifiable information (PII) recorded in application or system logs. In situations where numerous teams or staff members might be viewing PII, it is possible to record system or session information

A common technique to avoid privacy concerns when configuring proxies is to simply record system information instead of user login information.
for monitoring purposes into one table, with user-identifiable information associated with that session logged in a separate, more discreet table.

One common scenario for this type of “anonymous monitoring” is watching IP information for anomalous network activity and when such activity is detected and a specific incident confirmed, referencing DHCP tables to link the IP address to a specific user ID.

**PUSH DISCRETION AMONG SECURITY PERSONNEL**

In addition to selecting and configuring security solutions in a manner that supports both security and privacy efforts, you should also educate security personnel on appropriate skills and techniques. Even though it may seem obvious that security staff be ethical and discreet when performing monitoring and investigative tasks, it is not unusual for security staff to take liberties when communicating case details among themselves. That collaborative spirit can sometimes lead to eventual over-communication of details between security personnel and other teams or individuals within the company.

To help combat privacy disclosures within the organization, periodically educate staff on the importance of keeping PII related to security monitoring or investigations on a need-to-know basis until the appropriate time. In most cases the ideal situation would be to suppress information about an event or case involving PII until HR or the legal department needs to be debriefed.

In addition to educating personnel on discretion, it is also worth reviewing your incident response plan and evidence gathering policies and procedures to ensure they adequately limit PII access to appropriate incident response personnel.

As individual concepts, privacy and security are of paramount importance in today’s business world. In certain situations, however, you may find that they have opposing interests. With assistance from your legal counsel, proper tuning of security platforms and education of personnel, you will find that most conflicts can be avoided to help fully satisfy both security and privacy objectives. —Jeff Jenkins
End-to-End Encryption at the Forefront of Privacy vs. Public Safety Debate

**JUST A FEW** days after deadly attacks in Paris, Beirut and other cities, U.S. Central Intelligence Agency Director John Brennan grimly painted his view of the government surveillance landscape in the age of global terror.

During a press conference following the Paris attacks, Brennan referred to new challenges governments face when monitoring potential terrorists. These complications stem from **Edward Snowden’s NSA disclosures**, unease from legislators and the general public over the increasing intrusiveness of government surveillance, and—as current investigations into the Paris attacks are **bringing to light**—end-to-end encryption technology’s role in the war on terror.

**End-to-end encryption**, or E2EE, is the process of encrypting data—including text and email messages and video chats—at rest and in transit without third parties being able to access it. The data is decrypted only once it reaches its destination endpoint. The technology has become widespread as an increasing number of U.S. companies produce **intellectual property** such as product designs and concepts, as opposed to hardware or material goods. The use of E2EE has also played a significant role in how **technology companies like Apple differentiate** themselves with consumers who increasingly seek devices with features to protect against myriad cybersecurity threats and governments’ prying eyes.

But the pervasiveness of E2EE technology means that the bad guys also have access to it. There is no conclusive evidence by French and American officials on the role E2EE played in the recent terrorist attacks, but the ongoing debate between government intelligence agencies and Silicon Valley over the extent of government surveillance and **how encryption can hinder those efforts** has nevertheless been rekindled.
In the middle of this debate, many companies find themselves between a rock and a hard place: How can they protect their intellectual property and keep customer data private, but at the same time help law enforcement facilitate surveillance and investigations to keep the public safe from cybercrime and terrorist threats?

The answer is certainly not clear-cut. Even before the Paris attacks renewed the encryption debate, a panel of experts at the recent Advanced Cyber Security Center’s (ASCS) conference in Boston discussed its merits from a business perspective.

“If [intellectual property] is what you are producing, then you have to protect, and you have to protect everywhere. You have to protect the private cellphone as well as the cellphone that somebody is using for their work,” said panelist Susan Landau, professor of cybersecurity policy at the Worcester Polytechnic Institute.

There’s also the importance of customer trust, a necessity for global tech companies like Cisco.

“The ability to differentiate based on trust is really important for us—trust in the capabilities ... of our technology. If we are competing solely on cost, we will often lose because there are competitors that are able to drive down costs in ways that we might not be able to compete with,” said panelist Eric Wenger, director of cybersecurity, privacy and global government affairs at Cisco.

**ENCRYPTION AND ‘GOING DARK’**

To Cisco and its counterparts, there’s a tremendous economic benefit to the widespread use of encryption and other security technologies, Wenger said.

But end-to-end encryption comes with a price. One phenomenon that has resulted from the widespread use of encryption is what the U.S. Federal Bureau of Investigation calls “going dark,” or the increasing difficulty of law enforcement to access data and information on companies’ networks even when those agencies have the legal authority to do so.

Going dark puts public safety at risk, said James Baker, another ASCS conference panelist and the general counsel to the FBI.
“The expectation is on the FBI ... to have a zero failure rate when it comes to terrorism; we should not have a terrorist event in the United States,” Baker said. “That’s why, when we have dark corners where we can’t conduct surveillance—where the bad guys inhabit—that’s what freaks us out.”

One major “dark corner” the FBI has in its sights is the use of E2EE platforms by the Islamic State of Iraq and the Levant (ISIL), one of the most powerful extremist insurgent groups in the world. ISIL uses public, transparent channels such as social media platforms to communicate with potential recruits, and the group moves communications to encrypted networks once strong contenders have been identified.

“They switch to end-to-end encrypted platforms intentionally because they know the governmental entities can’t conduct surveillance on those things. That’s where they have their more operational conversations,” Baker said.

SPLIT-KEY AND KEY ESCROW ENCRYPTION

Despite the obstacles, Baker said that he and his colleagues understand that encryption is necessary because they don’t want to increase cybersecurity risk.

To address this dilemma, the U.S. National Security Agency (NSA) has proposed two technical solutions: split-key encryption and encryption using a method called key escrow. In the first technique, also known as “secret sharing,” data can only be decrypted by combining several keys after distributing access to more than one key holder, including the FBI (the user is able to access the data independently). In the latter, data can be decrypted with multiple keys, one of which is stored apart from the user—possibly by a government agency.

The proposals, however, have many experts and tech companies doing a double take. One of the issues with split-key and key escrow approaches is the sheer technical complexity of

One major ‘dark corner’ the FBI has in its sights is the use of E2EE platforms by the Islamic State of Iraq and the Levant (ISIL).
creating such systems while still keeping them secure.

“You can’t imagine the UN holding a split key. [And] the complexity of having 165, 200 nations, each with access to keys, is just unimaginable,” said Landau, adding that errors and flaws are still found even in existing protocols for establishing keys, such as the Advanced Encryption Standard.

Cisco’s Wenger also brought up the complexity problems of architecting a key escrow-based solution, especially because of the many moving pieces it involves.

“If we were able to engineer a mechanism where we could split a key and have a third-party escrow, and the U.S. government can come in and ask for it when they need it, the next thing that would happen is that the Chinese, the Russians, the Indians, the Brazilians—you name it—would come and ask for the same solution,” he said.

Furthermore, not only would split-key and key escrow encryption make systems more difficult to secure because of this complexity, but implementing these techniques could put U.S. companies at a competitive disadvantage to their international counterparts, Wenger added.

Once customers find out that their data is accessible either by key escrow or split keys, “it’s very likely that consumers could easily shift to other technologies that have the same functionality, or layer on their own open source messages for doing it as well,” he said.

—Francesca Sales
Businesses Weigh Security Pros and Privacy Cons of Sharing Threat Information

Rod Dykehouse doesn’t think cybersecurity is a fair fight. Like other CIOs, he sees more and more attacks coming from organized enemies like criminal syndicates and foreign governments.

To help even the odds, Dykehouse said he’s willing to work with the federal government, sharing information back and forth to more quickly identify and more effectively guard against cyberattacks.

“The cybersecurity attacks that are occurring are increasingly complex and sophisticated, and that, in my opinion, is an unfair fight,” said Dykehouse, CIO at Penn State Hershey Medical Center and College of Medicine. “If we have to figure this out on our own, we will lose the war before it’s begun. But by sharing, we can address this together.”

But Dykehouse also stressed that he isn’t giving the government unfettered access to his systems.

“We’re trying to make sure we’re protecting not only our networks, but also the privacy and confidentiality of the information with which we’re entrusted,” he said. “But we’re not opening the gates to them.”

NEW LAWS SPARK DATA SHARING DEBATE
Congress is expected to enact a new law creating a system that enables private entities and the federal government to share cybersecurity information. But the move is controversial and has many IT and cybersecurity leaders weighing the benefits of sharing that information against safeguarding the data confidentiality.

The U.S. Senate passed the Cybersecurity Information Sharing Act (CISA) on Oct. 27 with a 74-21 vote. Now leaders from the Senate and House, which passed its own cybersecurity sharing act, will have to work out differences between the two versions before they can move
Congress is expected to enact a new law creating a system that enables private entities and the federal government to share cybersecurity information.

“It’s a vehicle to help ensure that when there are attacks, others will know about them and know about them before they impact them, and I think the benefits far outweigh the risks in being able to help organizations,” he said.

Some IT organizations have also come out in favor of the law. For example, the College of Healthcare Information Management Executives, of which Dykehouse is an active member, and the Association for Executives in Health Information Security announced their support after CISA’s passage.

With passage of this new law expected, enterprise IT leaders will have to determine
whether they want to share information and if they do, how they’ll share that data while also protecting private information and meeting existing privacy laws.

“The concerns that privacy groups are voicing is that there isn’t enough details around what’s being shared. There are concerns about what data is going to be shared,” said Timothy Ryan, head of cyber security and investigations practice at Kroll, a provider of risk solutions.

THE COSTS—AND RISKS—OF CYBER THREAT INFO SHARING

Ryan said, ideally, private entities and the government would share cybersecurity threat indicators in an automated system. The information should flow back and forth in near real-time, with systems that automatically analyze threat potentials so IT and security staff only react to alerts, he added.

Most companies, however, do not have the systems in place for that sophisticated, automated level of sharing, he and others said, so more will have to be done manually. And because decisions on what will ultimately be shared rests with individual organizations, many businesses remain fearful about exposing private data or opening themselves up to other liabilities. Lawyers, consultants, IT professionals and security leaders said companies are concerned that if they share cybersecurity threat indicators, they risk drawing public attention to their cybersecurity vulnerabilities or the fact that they were hacked.

They also worry that by sharing their cybersecurity information, they open themselves up to government scrutiny that could find violations of other laws such as the Health Insurance Portability and Accountability Act. (Although privacy groups charge that the measure, which grants some immunity to organizations sharing cybersecurity data, will actually give companies a pass if they’re found lacking in such areas.)

Companies also fear that they face legal risks for agreeing to share information that potentially violates privacy law. They could simultaneously open themselves up to lawsuits from others by not participating in this sharing ecosystem: For example, companies could be sued for negligence by not doing all they
could to prevent a cyberattack, said attorney Julia B. Jacobson, a partner at McDermott Will & Emery LLP, a practice that focuses in part on privacy and data protection law.

Companies fear the legal risks for agreeing to share information that could violate privacy law.

As the proposed law stands now, private entities are not required to share their cybersecurity information. If they opt to participate and share, they’re asked to share threat indicators such as suspicious domain names or file names. However, Brown, Jacobson and others said companies may end up sharing more than that, including personally identifiable information (PII). Because CISA calls for sharing threat-related information, they said some companies could deem PII and other confidential or proprietary data as such.

“The complexity of the cyberattacks demands a great deal of information to analyze,” said Christos Dimitriadis, the international president of trade group ISACA and group director of information security at the Greek company INTRALOT.

But he, like others, said companies must implement strategies that can fulfill that need against the continuing need to keep confidential and proprietary information private.

“This is a balance that any organization should maintain,” he said. —Mary K. Pratt
JEFF JENKINS is a regulatory compliance, information security and risk management expert and currently the director of cybersecurity at Travelport LTD. Prior to his role with Travelport, Jenkins served in security executive/leadership roles for a number of private and public sector organizations including Cbeyond, Equifax, The First American Corp., S1, Georgia’s Dept. of Human Resources, and Cobb County Public Schools. He currently holds CISSP, CISA, CISM and CGEIT certifications.

MARY K. PRATT is an award-winning freelance journalist based in Massachusetts. She has covered various subject matters, ranging from community news to fashion to health and fitness. Her work has appeared in numerous publications, including newspapers, magazines and trade journals. She currently focuses her coverage on business management and information technology topics.

FRANCESCA SALES is site editor for SearchCIO and SearchCompliance. Before joining the CIO group, she was a copy editor and SEO specialist for TechTarget. She was also assistant site editor for SearchVirtual Storage and SearchITChannel. At Northeastern University, from which she graduated in 2011 with a bachelor’s degree in English and linguistics, Sales contributed to The Huntington News and worked as a writing consultant for the English department.