The Next Move

Regulatory and policy developments in tech—January 2023

EU's DORA looms large for financial firms, tech vendors

By Shawn Lonergan, Cyber, Risk & Regulatory Principal, and David Stainback, Cyber, Risk & Regulatory Partner 02

Generative AI tools push new boundaries for responsible AI

By Ilana Blumenfeld, Responsible AI Lead, PwC US Innovation Hub, and Joseph Voyles, Principal, PwC US Innovation Hub 07

Consumer product labels for cyber safety: Prepare to disclose

By Matt Gorham, Cybersecurity & Privacy Innovation Institute Leader, and Shawn Lonergan, Cyber, Risk & Regulatory Principal 10

Quantum leap in cyber risk spurs readiness push

By Matt Gorham, Cybersecurity & Privacy Innovation Institute Leader, Prakash Venkata, Cyber, Risk & Regulatory Principal, and Petar Petrov, Cyber, Risk & Regulatory Director 14

pwc

EU's DORA looms large for financial firms, tech vendors

By Shawn Lonergan, Cyber, Risk & Regulatory Principal, and David Stainback, Cyber, Risk & Regulatory Partner

The issue

The European Union is preparing to impose rigorous standards for operational resilience on its financial sector. But don't think this is just an EU issue — or, for that matter, a financial services issue.

The Digital Operational Resilience Act (DORA), which entered into force on January 16, is designed to protect the EU's financial sector against severe operational disruption. Following a two-year implementation period ending January 2025, DORA will impose far-reaching requirements for operational resilience on financial services firms — including banks, investment firms, insurance companies, brokers and credit rating agencies — as well as their critical service providers.

This last part is particularly noteworthy. For the first time, information communications and technology (ICT) providers that serve financial firms (e.g., providers of cloud services, software, fraud management services, penetration testing, information management systems and payment solutions) will be directly regulated by EU financial services authorities.

The regulator's take

The new regulation shifts the focus from only addressing a firm's financial resilience to also enabling it to maintain resilient operations when faced with severe disruption. The measure aims to confirm that all financial sector participants have safeguards in place to mitigate cyberattacks and other risks, such as supplier failure, service deterioration and concentration risk.

DORA sets uniform requirements for the security of network and information systems of almost all financial entities operating in the EU, as well as their critical vendors that provide ICT-related services such as cloud platforms, software products, data analytics and payment solutions.

DORA's foundation for operational resilience. The framework has five pillars.

ICT risk management	Incident reporting	Resilience testing	ICT third-party risk management	Information sharing
Governance and control framework for ICT risk management	Process for monitoring and logging ICT-related incidents	Annual testing of all critical ICT systems	Integration of third-party risk in ICT risk management framework	Voluntary sharing of cyber threat information and intelligence with other financial firms
Digital resilience strategy for implementing ICT risk management framework	Initial, intermediate and final reports on ICT-related incidents	Testing requirements proportionate to firm's size, business and risk profile	Contractual requirements and reporting of outsourcing register (including intra-group services)	Sharing arrangements compatible with data-protection and antitrust rules
Systems and tools to mitigate ICT risk	Implementation of a root-cause analysis following cyber incidents	Advanced threat-led penetration testing every 3 years	Reporting of changes in use of critical ICT services	
Business continuity policies and disaster recovery plans	Identification and reporting of required improvements	Collaboration with ICT providers	Assessment of ICT concentration risk and sub-outsourcing	
Ongoing monitoring of ICT risks and anomalous activities			Direct oversight of ICT third parties	
			Contract suspension or termination through supervisory authority	

In short, financial institutions will need to show that they're in control of their supply chain and third-party risks. At the same time, ICT providers that serve the financial sector will need to improve their own operational resilience.

Focus on ICT services. DORA's approach to ICT providers goes beyond third-party risk management. Financial institutions will need to conduct due diligence on prospective ICT providers and audit existing providers for suitability. They should rethink their service-level agreements with these vendors. Does the contract include adequate incident-reporting mechanisms and termination clauses? If your ICT provider is deemed critical, the firm will also need a mitigation backup plan in case the vendor goes down in a cyberattack. What are your firm's options in the event of a catastrophic service failure, regardless of the contract terms? What's the exit strategy?

As for ICT providers, those deemed critical will be subject to regulatory oversight that allows EU authorities to investigate and audit them, order changes to their security practices, impose penalties for noncompliance, and even require them to establish an EU-based subsidiary. This will likely push ICT providers to demonstrate the resilience of their own operations that support financial services firms, particularly where a client firm's "critical or important functions" are implicated.

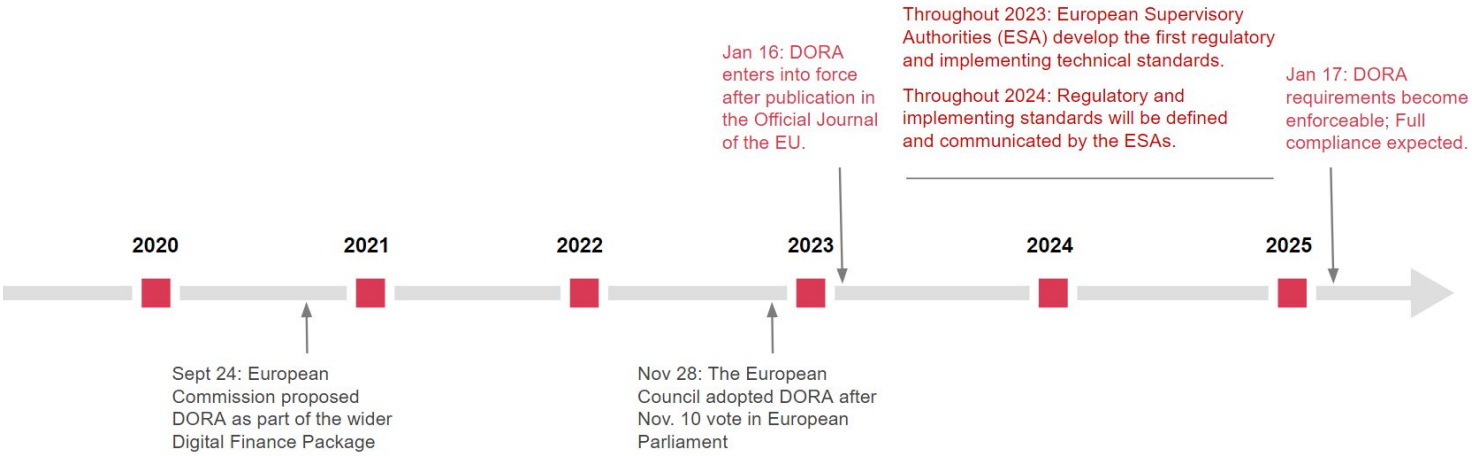
Penalties may be steep. Monetary penalties for financial institutions are not yet fixed. EU member states will formalize them in due course, and DORA also leaves the door open for potential criminal sanctions for violations.

Monetary penalties for critical ICT providers will be up to one percent of their average daily worldwide turnover in the preceding business year, applied daily until compliance is achieved, for a maximum of six months.

Technical standards yet to come. DORA will undergo a 24-month implementation period, with aspects that require national transposition to be passed into law by each EU member state. Concurrently, the relevant supervisory authorities, such as the European Banking Authority, the European Securities and Markets Authority and the European Insurance and Occupational Pensions Authority, will develop technical standards governing all aspects of financial services, including banking, insurance and asset management. These technical standards will take longer to finalize, leaving firms even less time to prepare.

Your next move

US businesses with ties to the EU financial sector need to understand their potential exposure. Now that DORA is approved, things will begin moving quickly. Get ahead of it before it gets you.



Financial institutions

1. **Are you a "financial entity" under DORA?** If so, begin charting a path to compliance.
2. **Do your programs align to DORA's pillars?** Map your risk management programs and assess for gaps. Identify opportunities to expand or refocus each program's scope to achieve compliance.
3. **How will you address gaps?** Work with risk management stakeholders to develop a plan for updating policies and controls to remediate gaps identified.
4. **What are your ICT-supported functions?** Identify all ICT-supported business functions, roles and responsibilities, the ICT assets supporting these functions, and their roles and risk dependencies.
5. **Do your service agreements measure up?**
    - Renegotiate contract provisions as needed to comply with DORA. Add, for example, robust incident-reporting mechanisms and terms allowing access, inspection and audit by the financial entity or an appointed third-party.
    - For critical service providers, consider flowing testing of controls downstream to your service providers.
    - Confirm that DORA-compliant terms are standard for all new supplier agreements.
6. **Are you monitoring vendor performance?** Strengthen performance monitoring as needed to help identify service deterioration and concentration risk within your supply chain.
7. **Is your testing adequate?** Review current resilience testing processes for completeness.
8. **Is your design approach compliant?** Implement a resilient design approach to new solutions that can mitigate supply chain risk.

Critical ICT providers

1. **Are you a critical provider?** Assess the likelihood of being designated a critical ICT service provider.
    - Even if that's unlikely, your customers may impose flow-through contract terms that require you to comply with DORA indirectly.
    - Talk with your customer base to better understand your DORA exposure and where you need to focus.
    - If serving the EU financial sector is or will become a business priority, all ICT providers — whether they're deemed critical or not — should consider taking the following actions.
2. **Which aspects of DORA apply to your services?** For covered services, create a roles and responsibilities matrix for your customers.
3. **Have you stress tested your services?** Perform stress testing to determine whether your services are sufficiently resilient under DORA and any flow-through contract terms.
4. **What about your suppliers?** Review your supply chain and identify which vendors are potentially covered by DORA.
    - Create a roles and responsibilities matrix.
    - Stress test critical suppliers further down the chain.
5. **Are you ready for inspections?** Prepare to participate fully in inspections, audits and other investigations by the designated financial services regulator.
6. **Do you have an EU-based subsidiary?** If not, recognize and plan for the potential risk of having to establish one.

Given the complexity of DORA and the view that regulator expectations will evolve as DORA is implemented, it's important to stay abreast of how your peers and ICT vendors are addressing the new regulation. For additional support, find the right professional services partner that can advise you through the journey to compliance.

Generative AI tools push new boundaries for responsible AI

By Ilana Blumenfeld, Responsible AI Lead, PwC US Innovation Hub, and Joseph Voyles, Principal, PwC US Innovation Hub

The issue

The democratization of AI is upon us as new generative AI tools put the power of AI into the hands of everyday users.

Users are eager to experiment with how these generative AI tools can write code, craft essays, create art, design blueprints, sketch package designs, create virtual worlds and avatars in the metaverse, troubleshoot production errors and so on. They're also learning how to refine their prompts or instructions to the tool, in iterative cycles, to achieve better results.

While the positive use cases for generative AI are staggering, there's also potential for misuse and harm. As users began exploring the new tool, for instance, many discovered they could use it to generate malware, write phishing emails and spread propaganda. The same tools also were found to "hallucinate" facts and reinforce perspectives from misinformation campaigns.

As generative AI becomes increasingly popular and widespread, questions about who is responsible for mitigating the associated risks will become unavoidable.

The regulator's take

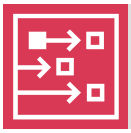
More than 800 AI policy initiatives are pending in 69 countries, but the application to generative AI models is not settled. The Biden administration's blueprint for an AI Bill of Rights, for example, can help organizations and developers manage risks for consumer-facing AI, but it doesn't address unique aspects of generative AI tools. The European Union announced its intention to regulate generative AI (included within general purpose AI systems), specifically around the data used to train them, under the EU AI Act.

Existing and proposed AI regulations today cover several specific use cases (e.g., data privacy, discrimination, surveillance), and specific decisions (e.g., hiring, lending, recommending on sites, public contracting), and most are enacted in response to the potentially harmful effects of AI on people and societies.

As users continue to discover new applications for these tools, new risks will likely emerge. The risks associated with generative AI are unprecedented and growing, but include:

- Deepfakes
- Phishing emails and social engineering
- Malware and ransomware code
- Plagiarism
- Copyright infringement
- Abusive or harmful content
- Disinformation and propaganda

Even without regulations to guide them, some companies are voluntarily adopting responsible AI models



Your next move

Capitalizing on opportunities while managing risks will require action from three stakeholder groups.

For developers and creators

- Apply responsible AI principles and practices.
  - Top platform owners have communicated their responsible AI strategies.
  - Google recently updated its search rater guidelines from E-A-T (expertise, authority and trustworthiness) to E-E-A-T, adding experience to its parameters for evaluating whether the company's search ranking systems are providing "helpful, relevant information."

- Prioritize nimble, iterative responses to events as they arise to complement robust internal practices. For example, the approach of some AI developers is to crowdsourcing use cases to disable answers for potentially harmful prompts in addition to their internal efforts to block harmful outputs.

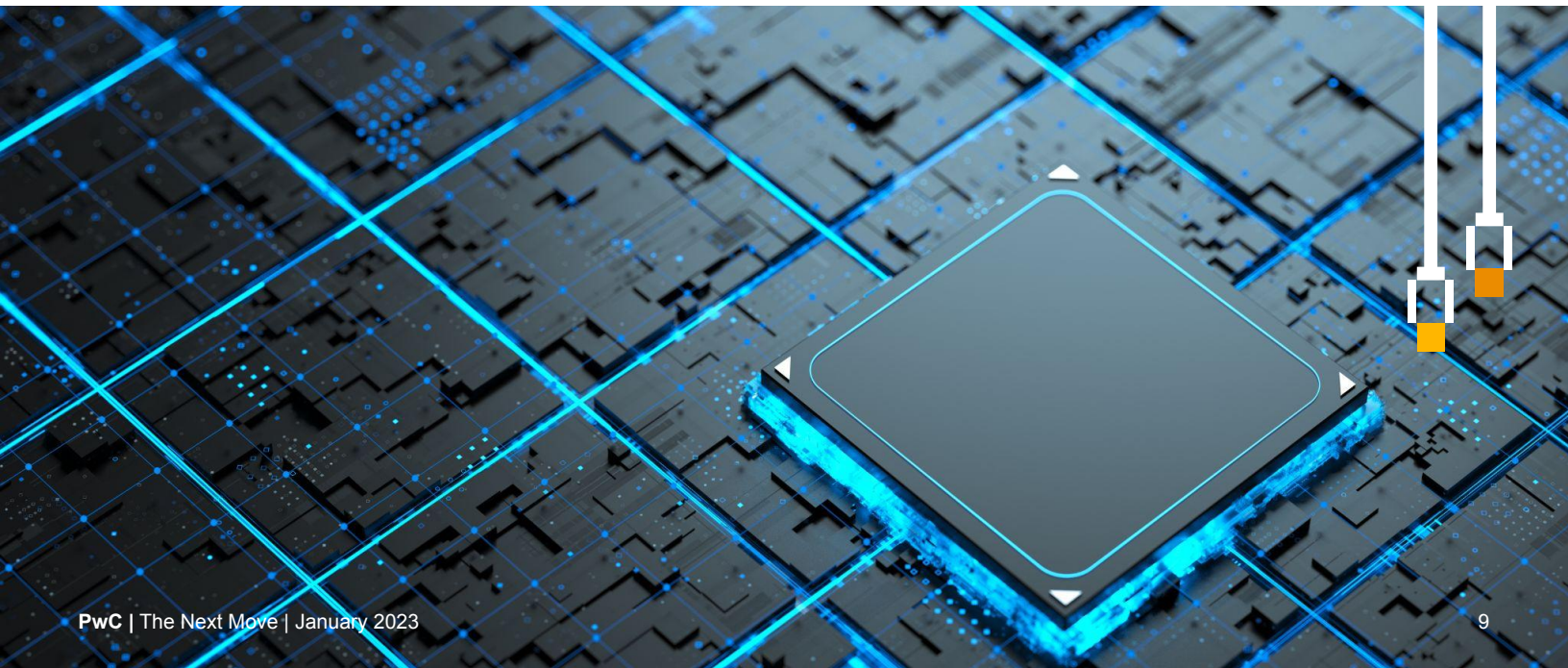
- Educate users on how to use generative AI. These tools are useful, but they're far from perfect. Individual and commercial users should have access to all the information about how they work.

For individual users

- Apply a critical lens to generative AI. Now that generative AI-created content lives alongside human-created content, be even more circumspect about taking any content at face value. Using generative AI tools may require additional research to verify the information it generates. Use emerging tools to identify AI-generated content and add citations whenever possible.
- Learn ways of maintaining integrity in the applications you work on. Generative models do not incorporate the concept of confidence in their responses and will attempt to make up an answer that better fits the prompt. In general, the default is to generate a response, true or not.

For commercial users

- Apply generative AI tools ethically but with the understanding that they come with potential risks. Lean on responsible AI frameworks to understand the potential shortcomings.
- Develop a policy around intellectual property related to products that are built from generative AI. Some models “reproduce” content that was present within the body of work they draw from, creating a situation where a licensed piece of code is incorrectly “generated” as a novel solution. Copyright protections are an important legal concern, and ambiguities around AI generated content as well as the data used to train these systems may impact the ownership and rights to use creative works.
- As with other AI, you may be using output from generative AI without even knowing it if your third-party vendors are doing so. Consider your third-party governance practices and how they can be augmented to provide additional guidance around creative applications of AI.



Consumer product labels for cyber safety: Prepare to disclose

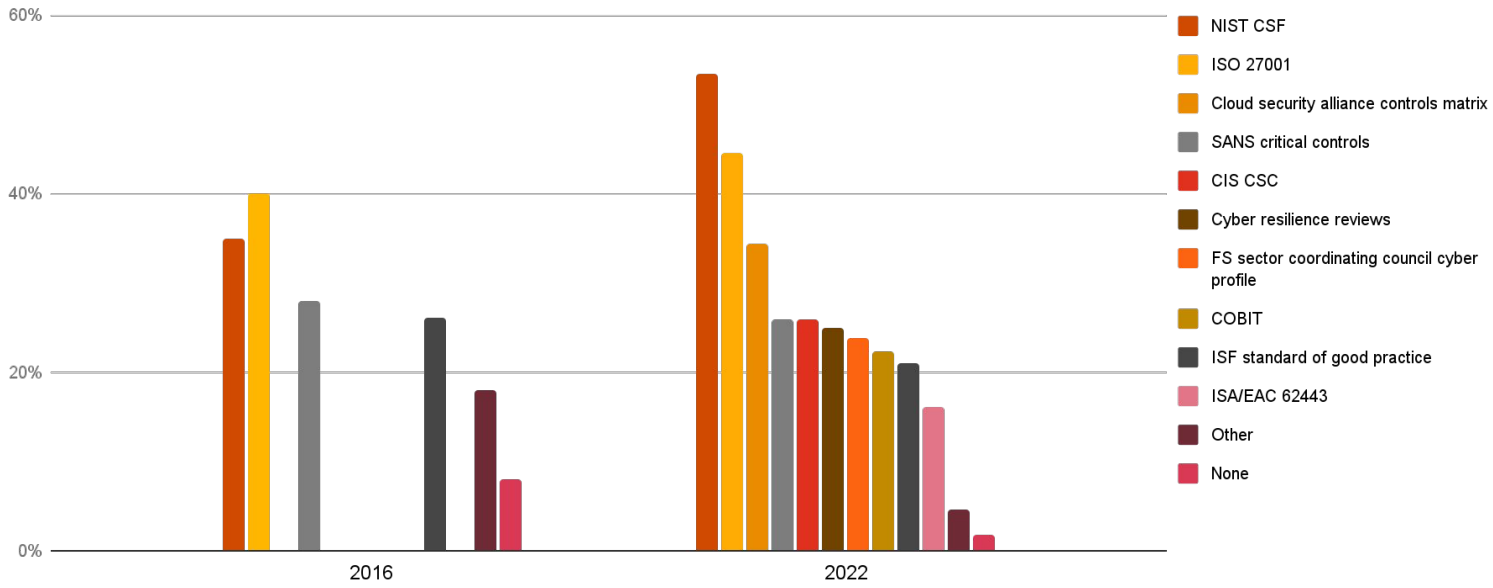
By Matt Gorham, Cybersecurity & Privacy Innovation Institute Leader, and Shawn Lonergan, Cyber, Risk & Regulatory Principal

The issue

Manufacturers and software companies continue to count on device interconnectivity — think the consumer-facing Internet of Things (IoT) and Industrial Internet of Things (IIoT) — for innovation and growth. Cybercriminals have similar plans, as malware attacks via commercial software and consumer-facing IoT devices are rising in tandem.

Businesses have increasingly adopted standards to better manage cyber risks. There are, however, no requirements that companies disclose their adherence to those standards. Consumers, B2B customers and shareholders have no easy way to know if a company is doing all it can to protect them.

The number of cyber standards and their use for managing risks have picked up significantly in recent years



Source: PwC, Global Digital Trust Insights, 2016 and 2022. CISO respondents. Survey was known as the Global State of Information Security Survey before 2018.

This is where cyber labels come into play. Like other consumer-facing labels such as the nutrition facts label on food packaging, the Energy Star label on electronics or the coming label for broadband internet, cyber labels are a way for IoT device manufacturers to provide *comparable* information in a *consistent* manner.

Success in a new era of transparency will likely hinge on better communicating how products are secure by design. Cyber labels can encourage competition on the basis of cybersecurity.

The regulator's take

The Biden administration has issued an executive order directing the National Institute of Standards and Technology (NIST) to develop guidance for two cyber labeling programs. In response, the agency published recommendations for potential labeling programs on cybersecurity capabilities for IoT devices and software development practices.

NIST drew from existing labeling programs such as Energy Star in developing its recommendations, rather than create a program from scratch. According to NIST's summary report, efforts to implement cyber labeling should:

- Encourage innovation.
- Be practical and not burdensome.
- Factor in usability.
- Build on national and international experience.
- Allow for diversity of approaches and solutions.

NIST recognizes that one size may not fit all when it comes to cyber labels and that multiple solutions might be offered by label providers in the near future. Its pilot program raised a number of issues in implementing a strategy for a cyber labeling program:

- A consistent label design.
- Efforts to educate the public.
- A broader consumer initiative to address cybersecurity issues.
- Flexibility for a wide range of products.
- Multiple scheme owners.
- Consistent and quality third-party assessments.
- Liability of key stakeholders.
- A common set of outcome-based cybersecurity criteria.
- A robust marketplace of standards.
- Mutual recognition of schemes between national economies.

In response to NIST's guidance, the White House is aiming to unveil an initial security label for IoT products with discussions beginning this spring.

Industry associations working on standards

According to the Connectivity Standards Alliance (CSA), around two dozen regulatory organizations representing more than 40 countries are developing IoT cybersecurity regulations or seeking certification to cybersecurity schemes for IoT products.

The CSA is working on solutions to cyber labeling and, more specifically, is building a common scheme and certification that will work globally by mapping and aligning three leading standards: NISTIR 8425 in North America, ETSI EN 303 645 in Europe, ISO 27402.

The Information Technology Industry Council recommends that a cyber labeling program should:

- Engage stakeholders, confirm clarity and balance responsibilities.
- Confirm the labeling format is flexible and the content is effective.
- Confirm labeling does not convey a false sense of security.
- Align with international standards and focus on features.

International cooperation gaining traction

The United States may join other nations, including Finland and Germany, in adopting Singapore's Cybersecurity Labelling Scheme. Launched by the Cyber Security Agency of Singapore in 2020, this voluntary program allows developers and manufacturers to demonstrate achievement of increasingly tighter security levels.

Level 1	Level 2	Level 3	Level 4
Meet baseline security requirements (e.g., unique default passwords, software updates, vulnerability disclosure policy)	Adherence to international standards	Adherence to the principles of security-by-design Software binaries assessed by approved third-party lab tests Absence of common software vulnerabilities	Resistance against common cyber attacks Undergone structured penetration tests by approved third-party test labs

Source: CSA Singapore, Cyber labelling scheme.

Additionally, Singapore has been working with industry and government partners to develop an international standard, ISO 27404, which defines a Universal Cybersecurity Labeling Framework. The framework is meant to serve as a guide for countries pursuing their own labeling initiatives for consumer IoT.

Your next move

One complication with cyber labels is the need for ongoing updates. A product could be considered secure one day and vulnerable the next due to the ever-changing nature of cyber threats. We expect the evolution from standards to labels to be a complicated, prolonged process.

But getting a head start may set organizations up for future success. Ask these three questions to assess your readiness for cyber-safety labeling.

1. **How well do you adhere to standards today?** Cyber labels are likely to follow the footsteps of existing cybersecurity standards discussed earlier. Examining your current standing with these standards may make the transition easier.
2. **Are you ready to communicate your adherence to these standards?** Some companies have already released their own guidelines for cyber labels. Google, for instance, published its five principles for IoT security labeling in November of 2022:
    - A printed label must not imply trust.
    - Labels must reference strong international evaluation schemes.
    - A minimum security baseline must be coupled with flexibility above it.
    - Broad-based transparency is just as important as the minimum bar.
    - Labeling schemes are useless without an adoption incentive.

    In the case of Apple's Privacy Nutrition Labels, disclosure of data collection practices is designed to improve user awareness and has been required of all apps available in the Apple App Store since 2020.
3. **Are you engaging with government and industry groups?** Actual implementation of cyber labels for any devices is likely years away and might be voluntary. However, if you manufacture certain devices, you might want to engage with the government to shape standards and cyber label requirements. Devices considered to be most at risk, including routers and home cameras, will likely be among the first to be labeled. So will devices that are produced by a handful of dominant manufacturers, which makes implementation quicker and more impactful.

(Two years after the Energy Star was introduced in 1992, more than 2,000 Energy Star qualified product models became available for sale; today more than 75,000 product models have earned the Energy Star. By 2019, for the first time, a majority of American households surveyed reported purchasing an Energy Star certified product.)

Quantum leap in cyber risk spurs readiness push

By Matt Gorham, Cybersecurity & Privacy Innovation Institute Leader, Prakash Venkata, Cyber, Risk & Regulatory Principal, and Petar Petrov, Cyber, Risk & Regulatory Director

The issue

A new US law requires federal agencies to protect sensitive information from "harvest now, decrypt later" theft by cybercriminals determined to unlock encrypted files accumulated over time with advances in quantum computing. The Quantum Computing Cybersecurity Preparedness Act, signed into law on December 21, 2022, requires agencies to migrate their information technologies to quantum-safe cryptography.

Able to solve complicated mathematical problems very quickly, quantum computers — using novel algorithms — might decipher today's computer system protocols and data encryption codes much faster than classical computers can.

Researchers have already used Shor's and Grover's algorithms, both quantum, to rapidly decipher the most rigorous encryptions used today. Twenty of 40 quantum experts queried expect the quantum threat to become "non-negligible" within 10 years, according to the Global Risk Institute's 2022 Quantum Threat Timeline report. Work is underway on quantum-resistant encryption, including the next generation public-key cryptography, according to mathematical physicist Spiros Michalakis, who spoke at PwC's Cyber Exchange in December 2022.

The regulator's take

Congress determined that the rapid progress of quantum computing suggests the potential for foreign adversaries to steal sensitive encrypted data today using classical computers, biding their time until sufficiently powerful quantum systems become available to decrypt it. A strategy for migrating the government's information technology to post-quantum cryptography is therefore necessary.

The new law establishes a timeline by which agencies are to inventory and list technologies vulnerable to quantum decryption and, once the National Institute of Standards and Technology (NIST) issues its quantum encryption standard, to begin migrating to those that are quantum resistant. The goal is to protect sensitive federal government information in the post-quantum age.

Within six months, the law requires the Office of Management and Budget (OMB) to issue guidance to agencies for compliance. Within one year, the OMB must require all agencies to prioritize their technologies for migration to post-quantum cryptography and to develop a plan for this migration.

A government-wide and industry-wide approach to post-quantum cryptography should, in Congress' view, prioritize developing applications, hardware and software that can be easily updated to support cryptographic agility.

Your next move

Contractors to federal agencies that handle sensitive information should begin now to prepare themselves for this change.

The law directs the OMB, in conjunction with the National Cyber Director and the head of the Cybersecurity and Infrastructure Security Agency, to "issue guidance on the migration of information technology to post-quantum cryptography."

The guidance is to include "a requirement for each agency to establish and maintain a current inventory of information technology in use… that is vulnerable to decryption by quantum computers; criteria to allow agencies to prioritize their inventory efforts; and a description of the information required to be reported."

All other businesses that process sensitive information may wish to prepare for the quantum threats as well, **but not at the expense of efforts to shore up your cyber posture today**. To prepare, we recommend several steps.

1. Engage with NIST for the latest updates on quantum-resistant algorithms and advisories on protocol changes.
2. Inventory your most sensitive and critical data that need to be protected in the next five to ten years. Assess the risk of your critical data being targets for "stored now, decrypted later" attacks.
3. Inventory all systems relying on cryptographic technology to prepare for the transition to post-quantum cryptography in the future. Develop processes to keep the system inventory up to date.

4. Identify where and why you are using public cryptography and mark those systems as quantum-vulnerable.
5. As you think about your transition, consider these criteria:
    a. Which assets and data are of high value to your organization.
    b. What data is your system now protecting, such as key stores, passwords, root keys, signing keys, personally-identifying information (PII) and sensitive PII.
    c. Communication with other systems inside and outside your organization.
    d. How long data needs to be secure.

Contact us

Why do we publish The Next Move?

Regulators and policymakers — keen to build new guardrails for a digital society — stand on largely unfamiliar ground. They often take different, sometimes contradictory, approaches because they have different missions and visions. At the global level, regulatory divergences reflect profoundly different value systems. Building trust in technology is complex work.

Through PwC's Next Move series, we can provide context to policy and regulatory developments in technology and tell you how you can get ahead of what might come next.

For additional information on our Next Move series, please contact:

Chris Pullano

Financial Services Advisory Partner

917 520 4447

christopher.pullano@pwc.com

Joe Nocera

Cyber & Privacy Innovation Institute Leader

312 925 6569

joseph.nocera@pwc.com

Michael Corey

Technology, Media and Telecommunications Partner

415 505 2482

michael.j.corey@pwc.com

Editorial team: Ted Trautmann, Cristina Ampil

© 2023 PwC. All rights reserved. PwC refers to the US member firm or one of its subsidiaries or affiliates, and may sometimes refer to the PwC network. Each member firm is a separate legal entity. Please see www.pwc.com/structure for further details.