CYBERSECURITY READINESS PODCAST SERIES

Episode 113

The EU Cyber Resilience Act Countdown: Why U.S. Companies Can't Afford to Look Away

with Mark Lambert, Chief Product Officer, ArmorCode

Host	Dr. Dave Chatterjee, Duke University
Guest	Mark Lambert, Chief Product Officer, ArmorCode
Topic Focus	The EU Cyber Resilience Act (CRA) — Vulnerability Disclosure Timelines, Compliance Scope, and Product Security Governance
Podcast Portal	https://www.cybersecurityreadinesspodcast.com/

Summary

In Episode 113 of the Cybersecurity Readiness Podcast Series, Dr. Dave Chatterjee is joined by Mark Lambert, Chief Product Officer at ArmorCode, to unpack the European Union's Cyber Resilience Act (CRA) and why U.S. companies cannot treat it as someone else's problem. Dr. Chatterjee opens with a scenario that captures the stakes: a mid-sized U.S. software company discovers one of its products is being actively exploited, investigates, patches, and notifies its customers within three days — a response most frameworks would call fast, but one that violates the CRA, whose clock for reporting an actively exploited vulnerability starts at 24 hours, not three days.

Lambert, who works daily with organizations on vulnerability management, explains that the CRA functions like GDPR for security: any software that ships into Europe, or that relies on supporting infrastructure serving European users, falls under its scope, and non-compliance carries fines of up to 2.5% of global revenue or €15 million, whichever is higher. The conversation walks through the CRA's three distinct notification clocks — a 24-hour early warning, a 72-hour full notification, and a 14-day final report after a fix becomes available — and dispenses with the idea that lacking sophisticated detection capabilities is a viable defense; the law expects secure-by-design practices and detection capability to already be in place before an incident occurs.

Analyzed throughout the episode through Dr. Chatterjee's Commitment–Preparedness–Discipline (CPD) Framework, the discussion also covers what well-prepared organizations are already doing — operationalizing vulnerability management programs and building real-time asset inventories — and closes with a shared view that regulatory pressure, while unwelcome, ultimately pushes organizations toward the security discipline they should be practicing regardless of legal mandate.

Discussion Highlights

The 24-Hour Clock: When Good-Faith Security Practice Becomes a Legal Violation

Dr. Chatterjee opens the episode with an illustrative scenario: a mid-sized U.S. software company discovers active exploitation of one of its products, does the right thing — investigates, patches, and notifies customers — but takes three days to do it. Under most frameworks, he notes, that is a reasonably fast response; under the EU Cyber Resilience Act, it is a violation, because the reporting clock for an actively exploited vulnerability starts at 24 hours, not three days.

> *That gap between what feels like good cybersecurity practice and what the law now requires is not really a story about bad intentions. It's a story about operational discipline that most organizations haven't built yet, and it's coming for a lot more companies than they think.*
>
> **— Dr. Dave Chatterjee**

CRA as "GDPR for Security": Why Scope Reaches Far Beyond Hardware Devices

Lambert frames the CRA as GDPR's counterpart for security: it converts vulnerability response from a business best practice into a mandatory product safety requirement, enforced through a CE marking that now applies to software as well as physical products. Scope extends well beyond internet-connected devices like thermostats to any software installed on hardware sold into Europe — laptops, browsers, gaming devices, and mobile devices — and the fines mirror GDPR's severity: 2.5% of global revenue or €15 million, whichever is higher.

> *I would summarize that the Cyber Resilience Act is kind of like GDPR, but for security, and it changes your vulnerability response programs from being a business best practice into a product safety issue that you actually require to have fully operationalized to do business in Europe.*
>
> **— Mark Lambert**

Beyond the GRC Team: Vulnerability Disclosure Becomes a Security Operations Problem

Lambert adds two further nuances to the scope question. First, it is not only the software running on a device in Europe that falls under the CRA — supporting infrastructure such as a backend data server, even one hosted far outside Europe, is in scope too, especially where data collection and processing are involved. Second, while much of the CRA reads like a governance, risk, and compliance (GRC) exercise around secure-by-design practices, the 24-hour vulnerability disclosure requirement is different: it is an operational security demand that GRC processes alone cannot satisfy.

> *GRC processes don't handle that kind of thing. Now your vulnerability management program is part of your business requirements for disclosure externally... so it's not just the governance or the GRC team's problem. It's the security operations team's problem as well.*
>
> **— Mark Lambert**

Three Clocks, Not One: Decoding the CRA's 24-Hour, 72-Hour, and 14-Day Timelines

Responding to Dr. Chatterjee's comparison to the seven-day incident reporting window referenced in a U.S. executive order, Lambert clarifies that the two are not an apples-to-apples comparison. The CRA actually runs on three separate clocks: a 24-hour early warning that starts the moment an organization becomes aware of an actively exploited vulnerability, a 72-hour deadline for a full notification with details on blast radius and affected versions, and a 14-day deadline for a complete report after a fix is released. He points to Log4j as a reminder that identifying the true blast radius of a vulnerability can itself take days — underscoring why the CRA's "best effort" requirement to continuously shrink these timelines, backed by real fines and market exclusion, gives it more enforcement teeth than most U.S. executive orders.

No "We Didn't Know" Defense: Secure-by-Design Is Not Optional

Asked directly whether a lack of sophisticated detection systems could excuse a delayed report, Lambert is unequivocal: the CRA requires secure-by-design practices and detection capability to be in place beforehand, so claiming unawareness is no more a defense than a driver claiming they weren't looking at the speedometer. He lays out the compliance timeline: full CE-marking submissions are due by December 2027, but the 24-hour vulnerability reporting requirement itself takes effect far sooner — September 11, 2026, less than 90 days from the recording of the episode.

> *The actual Cyber Resilience Act says that you have to have secure by design... As you're just saying, 'I didn't have the signal, so therefore that's a defense' — no. That's like, oh, I wasn't looking at my speedometer. No, that is not going to help you at all.*
>
> **— Mark Lambert**

The CPD Framework Meets Regulatory Reality

Dr. Chatterjee connects the discussion to his Commitment–Preparedness–Discipline (CPD) Framework, noting that regulations like the CRA make the case for commitment easier to sell to leadership. He stresses that commitment starts with engaging legal experts from the outset — alongside the security-by-design principle — so organizations understand which regulations apply to them and how to stay ahead of, or at least in compliance with, evolving requirements, rather than discovering obligations only after an incident.

Best Practices from the Field: Operationalizing Vulnerability Management and Asset Inventory

Lambert describes what well-prepared organizations are actually doing: building an operationalized vulnerability management program — detection signals paired with an orchestrated workflow that compresses the time between find and fix — and layering a real-time inventory and classification of deployed assets on top of it. Because SaaS products, browser

plugins, and mobile apps can have many versions live at once, organizations need to understand interdependencies between teams and products, as well as downstream risk introduced by open-source components and third parties, not just their own codebase.

Dr. Chatterjee adds that asset inventory monitoring has to be a continuous, real-time exercise rather than a periodic one, and that while remediation tools can automate patching, human oversight remains essential to confirm those automated systems are performing as expected.

The Reasonable-Effort Standard: Why How You Respond Matters More Than Perfection

Dr. Chatterjee raises a practical concern: despite best efforts, an organization can still be found non-compliant or still be breached. Drawing on conversations with legal experts, he notes that regulators and courts tend to be sympathetic to a "reasonable effort" standard — did the organization, given the resources available to it, genuinely do its best? Lambert agrees, framing this as the real spirit of the CRA: it is not about preventing every individual incident, but about whether an organization has an operational program in place and demonstrably improves it when gaps are found.

> *You can't use the do-nothing defense... but the best effort — at the end of the day, yes, companies get breached. It's about how you respond to something that's most important, and that I feel like that's really the spirit of the Cyber Resilience Act.*
>
> **— Mark Lambert**

Closing Reflections: Turning Regulatory Pressure into a Competitive Advantage

Dr. Chatterjee closes by reiterating that the CRA does not test an organization's documentation — it tests whether its vulnerability management program actually runs, which is why cybersecurity readiness has to be treated as a strategic, organization-wide priority rather than something outsourced or bolted on to satisfy a regulator. He shares a personal analogy from ninth grade, recalling a physics teacher whose exams demanded more than the assigned textbook could prepare students for; disliked at the time, that higher bar ultimately made students better prepared. He casts the CRA's architects in a similar light: unwelcome in the moment, but ultimately pushing organizations toward a stronger security posture. Lambert closes by noting that the CRA's reach is broader than most companies assume — even software with no physical form, like a password manager, falls under one of its highest risk classifications — and points listeners to resources ArmorCode has published on the CRA, including a self-assessment tool, as well as the Purple Book Community, which hosts active discussion on the CRA and on AI's growing impact on security.

The CPD Framework Applied to EU Cyber Resilience Act Compliance

Dr. Chatterjee maps his Commitment–Preparedness–Discipline (CPD) Framework directly onto the CRA compliance and product-security themes discussed throughout the episode.

CPD PILLAR	APPLICATION TO EU CYBER RESILIENCE ACT COMPLIANCE
COMMITMENT	Leadership treats CRA compliance as a strategic priority tied to product safety, not a paperwork exercise — engaging legal experts from the outset in developing and executing security strategy so obligations are anticipated rather than discovered after an incident.
PREPAREDNESS	Organizations build an operationalized vulnerability management program — detection signals, orchestrated workflows, and real-time asset inventory and classification — capable of compressing find-to-fix time enough to meet the CRA's 24-hour, 72-hour, and 14-day clocks.
DISCIPLINE	Detection, triage, and response run continuously and cross-functionally — legal, IT, and security working together — so the program survives leadership turnover and business pressure rather than being assembled from scratch when a regulator or customer asks.

Actionable Recommendations

RECOMMENDATION	DETAIL

Map Your CRA Exposure Now	Determine whether your products, and any supporting infrastructure such as cloud-hosted backends, fall under CRA scope — scope definition, including third-party and open-source dependencies, is where many organizations struggle first.
Build the 24-Hour Detection-to-Disclosure Muscle	Invest in automation and correlation tooling that can establish blast radius and get an early-warning notification out within 24 hours of becoming aware of an actively exploited vulnerability.
Track All Three Regulatory Clocks	Plan around the 24-hour early warning, the 72-hour full notification, and the 14-day final report after a fix — and treat "best effort" to shrink those windows as an ongoing obligation, not a box to check once.
Don't Rely on a "We Didn't Know" Defense	Secure-by-design practices and detection capability are expected upfront; lack of sophisticated monitoring is not a legal defense, and the 24-hour reporting requirement takes effect September 11, 2026.
Operationalize Vulnerability Management as a Control Plane	Move beyond point-in-time scanning to an orchestrated workflow with clear ownership that shortens the time between finding and fixing a vulnerability.
Build Real-Time Asset Inventory and Classification	Continuously track what is deployed, in which versions, and how products interconnect across teams — including third-party and open-source components — rather than relying on periodic reviews.
Engage Legal from the Start	Bring legal expertise into security strategy development early so regulatory obligations are anticipated and translated into terms the rest of the organization can act on.
Apply the CPD Framework to Sustain Compliance Under Pressure	Use Commitment to secure leadership buy-in and legal engagement, Preparedness to build response capacity, and Discipline to keep the program running through turnover and business stress.

Time Stamps

TIME	CONTENT
0:02	Introduction — Dr. Chatterjee's background and credentials
0:49	Host framing: the EU Cyber Resilience Act and the 24-hour reporting scenario; guest introduction
3:37	Mark Lambert's professional background and focus on vulnerability management
4:41	What the CRA requires and why U.S. and SaaS companies should care
5:05	The CRA as "GDPR for security" — CE marking and fine structure
7:42	Scope beyond the device: backend infrastructure and the GRC vs. security operations distinction
9:17	Comparing the CRA's 24-hour clock to U.S. executive order reporting timelines
10:50	The three CRA clocks: 24 hours, 72 hours, and 14 days after a fix
13:59	Is unawareness a loophole? The secure-by-design requirement
16:50	Key compliance dates: September 11, 2026 and December 2027
19:12	Comparable regulations in other regions and the business case for readiness
21:41	The CPD Framework introduced and applied to CRA compliance

25:36	Best practices: operationalized vulnerability management and asset inventory
28:51	Continuous asset monitoring and the role of human oversight
32:17	The reasonable-effort standard and the spirit of the CRA
33:03	Cybersecurity readiness as a strategic value proposition
38:19	The physics-professor analogy: preparation beyond the minimum
38:51	How Lambert first encountered the CRA and its broad scope
41:16	Closing thoughts from Mark Lambert: ArmorCode resources and the Purple Book Community
42:05	Special thanks and episode wrap-up

Memorable Quotes

> *That gap between what feels like good cybersecurity practice and what the law now requires is not really a story about bad intentions. It's a story about operational discipline that most organizations haven't built yet.*
>
> **— Dr. Dave Chatterjee**

> *I would summarize that the Cyber Resilience Act is kind of like GDPR, but for security, and it changes your vulnerability response programs... into a product safety issue.*
>
> **— Mark Lambert**

> *That's like, oh, I wasn't looking at my speedometer. No, that is not going to help you at all.*
>
> **— Mark Lambert**

> *You can't use the do-nothing defense... It's about how you respond to something that's most important, and that's really the spirit of the Cyber Resilience Act.*
>
> **— Mark Lambert**

Disclaimer

The information contained in this summary is for general guidance only. The discussants assume no responsibility or liability for any errors or omissions in the content of this podcast. The information is provided on an as-is basis with no guarantee of completeness, accuracy, usefulness, or timeliness. The opinions and recommendations expressed are those of the discussants and not of any organization.

Dr. Dave Chatterjee | dchatte.com | dchatte@gmail.com | linkedin.com/in/dchatte
© 2026 Dave Chatterjee. All intellectual property rights reserved. | cybersecurityreadinesspodcast.com