White Paper

HardenStance

Preparing for New Incident Reporting Requirements

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

CYBER THREAT ALLIANCE paloalto NETWORKS

November 2022

HardenStance
"Trusted Research, Analysis and Insight in IT & Telecom Security"

Executive Summary

- Mandatory cyber incident reporting is being extended to many more organizations. Those already subject to these regulations face new, more stringent, requirements.
- Engaging proactively with government agencies and your own incident response and legal partners will make mandatory incident reporting as frictionless as possible and allow you to derive maximum benefit from the process.
- Defining a 'material' incident for your organization and selecting appropriate incident response and legal firms are among the preparatory measures required.

New Incident Reporting Rules are in the Pipeline

Three of the examples of new legislation in the pipeline extend new rules to organizations that were previously exempt.

Government-imposed rules on incident reporting by organizations impacted by cyber attacks are not new – many critical infrastructure sectors have been subjected to them for decades. What is new, though, is the recent and marked acceleration in the rate at which governments are introducing new, more stringent, incident reporting rules; the widening of the scope of those rules to include new, previously unregulated industry sectors; and the broadening of the coverage of those rules to embrace smaller companies - not just the largest, dominant players, in those industries.

Five examples from the U.S, the UK, the EU and Australia are shown in **Figure 1**. In four cases, the driver for these new incident reporting requirements is national security in the form of the security of critical infrastructure. In the case of the fifth, the Securities and Exchange Commission (SEC) in the U.S, the goal is to give investors better transparency into the way companies are being run. The SEC now judges a public company's exposure to cyber risk to be so important for valuation assessments that investors have a right to know when a material cyber incident has occurred.

Whereas two of the examples cited are updating the rules applicable to sectors and organizations that are already subject to regulation, three examples of new legislation in the pipeline extend reporting rules to organizations that were previously exempt.

Figure 1: New Regulations Around the World Prescribing New Incident Reporting Requirements

Country or region	Legislative or regulatory body	New regulations or legislation	Affected organizations	New incident reporting rules (may be subject to change)	Likely date of impact
Australia	Dept of Home Affairs	SLACIP* Act	Providers of critical infrastructure	Submission of initial report within 12 hours	July 2022
Europe	European Commission	NIS2 Directive	Providers of critical infrastructure (Scope widened**)	Submission of initial report within 12 hours	2023
USA	Securities & Exchange Commission	Incident Disclosure rules (Amendment)	Any public company	Submission of initial report within 4 working days.	2023
USA	DHS/CISA	CIRCIA*	Providers of critical infrastructure	Submission of initial incident report within 72 hours.	2023
UK	DCMS	Consultation on cyber legislation	The suppliers to providers of critical infrastructure.	Rules for suppliers to providers of critical infrastructure.	2023/2024

* *Cyber Incident Reporting for Critical Infrastructure Act; Security Legislation Amendment Critical Infrastructure Protection*

*** As well as sectors covered by NIS1, NIS2 now covers postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers.*

Source: HardenStance

The EU's NIS 2 Directive widens the definition of critical infrastructure providers to include postal and courier services; waste management; manufacture, production and distribution of chemicals; food production, processing and distribution; manufacturing and digital providers. Driven by supply chain security principles, the UK's ongoing consultation proposes extending incident reporting requirements beyond critical infrastructure providers themselves to their suppliers. Most striking of all, the SEC's new rules apply to any public company, irrespective of size or sector. Not mentioned in **Figure 1**, but nonetheless very important, is the EU's Digital Operational Resilience Act (DORA). This expands the scope of incident reporting for the financial services sector, requires faster reporting and seeks to streamline the reporting process.

The metric that tends to get the most attention is the number of hours or days within which an initial report on a material incident must be reported as well as requirements to provide subsequent updates. But other rules are quite often being introduced or updated in parallel. These relate to things like a Board of Directors' oversight of cybersecurity risk; management's role in managing and implementing cybersecurity policy; and auditing of the amount of cybersecurity expertise among board members.

"We're from the government and we're here to help"

There are some entirely legitimate reasons to fear the impact of mandatory reporting. The wrong kind of disclosure can tip off attackers and exacerbate the harm caused.

U.S President, Ronald Reagan, famously said that "the most terrifying words in the English language are 'we're from the government and we're here to help'. It's easy enough for CISOs and business leaders to feel that way about having to comply with new or updated regulatory requirements during normal circumstances - or what cyber incident responders call 'peace time'. It's an even more natural response amidst the real-time fear, uncertainty and anger that arises when a potentially major incident has just been discovered. A new legal requirement to devote time to telling the government what's going on when business leaders almost certainly don't yet have an accurate picture themselves can feel like government is being anything but "helpful".

Albeit with variations between and within different regions of the world, government agencies are usually anywhere from somewhat to very helpful in helping victims recover, as well as applying what they learn from an incident to support other stakeholders. Leading incident response companies routinely attest they would not be able to minimise the blast radius of an attack to the extent that they often can without support from government agencies, including information sharing and other forms of collaboration with government agencies in other countries. Governments just want all stakeholders – including government itself – to continue improving on the way they respond, and the outcomes that result from it.

The last thing you want to do is tip an attacker off

There are some entirely legitimate reasons to fear the impact of mandatory reporting. Most obviously, the wrong kind of disclosure - too much information, the right information released too soon or wholly unnecessarily; or the right information shared with the wrong people – can tip off attackers mid-attack and exacerbate the harm caused to the organization itself and potentially to others too. Equally, some concerns arise from a lack of familiarity with the rules. For example, in most countries incident reports typically do not automatically trigger law enforcement to open a case. That said, the fact that a case isn't opened immediately does not mean that the authorities are not taking any action at all - or that they won't open a case after further investigation.

What all this points to is the need for business leaders and CISOs to take a more nuanced view of new incident reporting requirements than they might first be inclined to. They should strive for a balanced understanding of how to benefit from new incident reporting rules while mitigating the potential risk that arises with it. And they should take steps to make compliance as beneficial, friction-free and low cost to their business as possible.