White Paper

HardenStance

Preparing for New Incident Reporting Requirements

By Patrick Donegan, Principal Analyst, HardenStance

Sponsored by

November 2022

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.

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.

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

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".

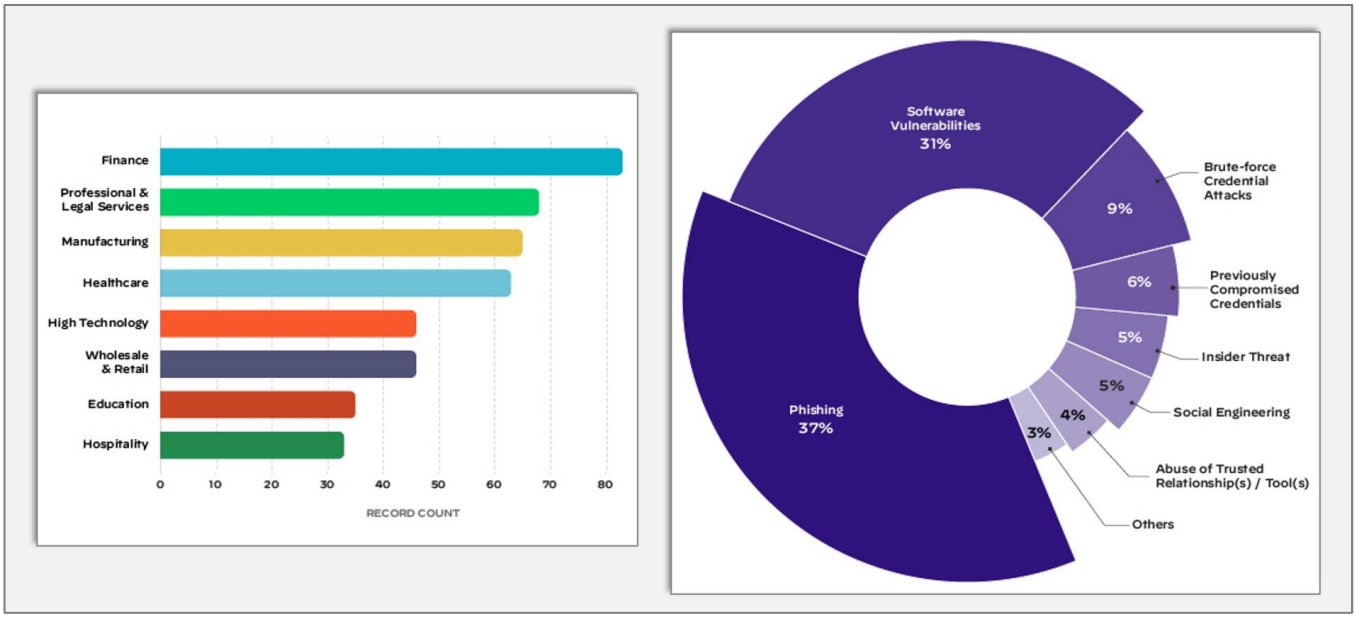
Albeit with variations between and within different regions of the world, government agencies are usually anywhere from somewhat to very helpful in helping victims recover, as well as applying what they learn from an incident to support other stakeholders. Leading incident response companies routinely 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.

Figure 2: Industries Most Affected by Cyber Attacks and Most Popular Suspected Means of Access



Source: Palo Alto Networks Unit 42 "Incident Response Report 2022"

"Benefits? What Benefits?"

There are three distinct outcomes from more stringent mandatory incident reporting that should be welcomed by company boards, CISO teams, and investors alike.

1. **Access to better, government-mediated, threat intelligence**. A number of government regulatory agencies around the world have become pretty good at managing a life cycle that starts with mandatory incident report inputs from victims and evolves into threat intelligence outputs that can benefit many stakeholders. The potential for insights from an incident reported by a competitor or peer organization to reach your own CISO team in time to implement protections before you suffer the same fate is self-evidently hugely valuable.

   Recognizing that potential of an efficient incident reporting and threat intelligence sharing model – jointly managed by government and the private sector – should drive two take-ways. First, no organization can reasonably expect to benefit from a well-run, secure, threat intelligence-driven ecosystem without itself having to report on its own incidents. Second, perhaps less obvious, is that where government agencies are flawed in their management of the threat intelligence ecosystem, organizations that have the resources should be looking to help drive improvements.

By placing requirements on a company's Board, incident reporting rules make the Board more directly accountable for an organization's cybersecurity policy.

2. **Making the Board of Directors more directly accountable for cyber security.** By placing requirements on a company's Board, incident reporting rules make the Board more directly accountable for an organization's cybersecurity policy. It changes the legacy 'bottom-up' dynamic of cybersecurity in which a CISO communicates upwards around what he or she is doing and makes requests of the board accordingly. Incident reporting rules drive more of a two-way dialogue. The Board can no longer view cybersecurity as something that it can delegate to the CISO team and participate in passively, without taking much responsibility.

3. **More informed government policymaking.** Part of the reason cybersecurity policy can be flawed or lag far behind real world market and technology developments (or both) is that governments lack sufficient data on cyber attacks on which to base policy. This benefit isn't as immediately tangible as the others but improving visibility into cyber incidents should give governments access to much better data about incidents which in turn should drive better government policy.

Preparing For New Rules: General Principles

In preparing for new rules, there are four core principles to have in mind:

1. **Take a breath:** Between the months building up to the release of draft legislation or regulations, a subsequent consultation period, and an often phased implementation, there's plenty of time to prepare for the new regime.

2. **Don't just learn about the new rules – shape them.** Smart governments engage in a consultation period after the publication of a first draft of new rules. At minimum these public consultations provide an opportunity to learn about what's coming down the pipe. That can entail reading published comments and submissions. Or it can mean attending public consultations in-person, which also creates opportunities to network and learn from peers who are navigating the same challenges. Better still, these are opportunities to actively contribute to public consultation and shape the regulations. If draft rules do not specify that submission of reports will be possible via a highly secure on-line portal so as to allow deadlines to be met, then use a public consultation period to lobby for that to be introduced. If draft rules propose that submitting a report triggers a mandatory obligation to also report to multiple other agencies, consider pushing back in favour of leaving businesses to make their own decisions as regards any other reporting obligations.

When the clock is ticking, you have a far better chance of achieving your goals within the law if your organization is at least somewhat familiar with the relevant agencies.

3. **Get familiar with the people you will submit reports to.** There's a world of difference between a dry legislative or regulatory tome and the individual human beings involved in enforcing it. So get familiar with Maria at your industry regulator; Jing at the financial services regulator, Rajesh at your national cyber security agency and David in law enforcement. Assemble their contact details in one place – ideally their mobile numbers as well as their departmental phone numbers.

   Then when the time comes, you'll be able to recall the statement one of them made in a speech a few months ago; the comment another made to you during the break at another conference; maybe even the remarks another made in a private meeting. These opportunities provide critical colour and context on how the new rules will be applied in practice. They will give you insight into the flexibility, variability and room for negotiation there is likely to be - or not likely to be - in terms of what needs to be reported, when and who to, depending on the specifics of the incident.

   When the clock is ticking, and decisions need to be made rapidly under often intense pressure, you have a far better chance of achieving your goals within the law if your organization is at least somewhat familiar with the relevant agencies. Many - arguably most - people who have experienced a serious cyber incident will tell you that time invested familiarizing yourself with these individuals may not appear to be very well spent before an incident occurs. But when it does happen, you'll either congratulate yourself for having done it – or curse yourself for not having done it.

4. **Keep Cost Containment Front and Centre.** The 2022 'Cost of a Data Breach Report', featuring research by the Ponemon Institute, states that organizations with an Incident Response (IR) team that tested its plans saved an average of $2.6 million compared with those that didn't. It may sound obvious that containing costs is a core principle of incident management and incident reporting but some of the key factors that determine those costs are not. Internal friction within your own organization is one. The less prepared, the less well-rehearsed, the organization is for incident management across all its key stakeholder departments, the greater the likelihood of initial reporting decisions being made too quickly - and better reporting ones only being made much later in an effort to compensate for those earlier bad ones. Internal friction in responding doesn't just impede an organization's ability to minimize the blast radius of an incident. It also drives up the costs of the final bill from reporting, response and recovery partners such as third party IR partners and law firms.

Preparing For New Rules: Specifics

So much for the general principles to bring to incident reporting – what about some specifics? These below are some important practical steps organizations can take to ensure they can report an incident within the timeframe required, with the highest possible level of accuracy, and with the necessary safeguards to ensure that neither the information itself, nor the way it is shared, puts the organization itself or others at risk.

1. **Arrive at a definition of a 'material incident'.** It's only incidents that are considered "material", "significant" or "substantial" that governments want reported. At a high level, the qualifying criteria typically entails one or more from four impacts – financial loss; exfiltration of data (customer information, trade secrets, or intellectual property); operational disruption; and damage to brand or corporate reputation. Exactly what quantitative or qualitative threshold of damage has to be crossed to meet a given country's definition is usually up to each organization to define itself. It's in their nature that such rules and regulations that are designed to be universal don't map exactly to any one organization**.**

   Ultimately, if you don't know what qualifies as a material incident, how can you tell whether or not you need to report it?

   The chosen definition must nevertheless broadly align with a regulator's stated expectations, as well as an organization's own operational risk register. With this in mind, and with support from external guidance, organizations must leverage the cold light of day – "peace time" – to arrive at their own clear definition of what they consider a 'material incident'. Ultimately, if you don't know what qualifies as a material incident, how can you tell whether or not you need to report it? When a potentially material incident occurs, the clock starts ticking on your potential obligation to report it. Determining whether a "material" threshold has been crossed can be very challenging. At that point, you don't want to waste precious time arguing about what that threshold should be.

2. **Review and refine your incident response plan.** Your incident response plan needs to have your approach to meeting incident reporting requirements embedded in it. The names of all relevant agencies, contact persons and their contact details need to be listed and that list needs to be regularly reviewed and updated. The organization's definition of a 'material incident' needs to be included. Hard copies of the incident response plan need to be kept along with digital copies backed up on isolated devices – otherwise a ransomware attack could end up encrypting your only digital copy so that you're not even able to access your response plan when the time comes. The response plan needs to be practised with the participation of senior management in half-day or one-day rehearsal exercises twice a year.

3. **Review your key third party partnerships.** When you think you might have to report an incident, or you're already clear that you do have to, you won't want expert partners around you that have some relevant experience or are merely "good enough". You will want really good partners around you – people that inspire confidence. So when it comes to lawyers or external counsel, you will want a law firm that is experienced in data breaches. More than that, you will want a firm that is familiar with dealing with breaches in your sector of industry. Ideally, they will also know the relevant agencies that must be reported to, how to engage with them, and be familiar with their representatives. It's not uncommon for large organizations to hire multiple law firms for their different specializations. Smaller organizations need to be similarly wary of relying on just one generic law firm for cyber incident response. They should have an appropriately specialized law firm lined up - ideally one that is at least somewhat familiar with their business - for when the time comes.

Figure 3: The Four Categories of 'Material' Incident

Source: HardenStance ** 'Material', 'significant' or 'substantial'*

Incident response companies also tend to have specializations. If your cyber risk assessment points to your organization being especially vulnerable to ransomware, then your incident response partner should have a lot of experience dealing with ransomware attacks. A company that can point to previous experience responding to multiple breaches in your specific sector of industry may also be a better partner than one with no experience at all in your sector.

You will want the very best possible expertise around you so identify who can provide that ahead of time.

Your law firms and incident response companies are the ones you need to help you navigate a path through the minefield of legal obligations and potential remediations over days, weeks, maybe months. They're there to help you identify, understand and evaluate all the many trade-offs in different kinds of risk to the organization as you navigate that path. They will help you make the best possible decisions on what information to share, who with, how and when. They'll help weigh up your options on which systems to shut down, which to restart, and when. You will want the very best possible expertise around you so identify who can provide that ahead of time.

4. **Pre-populate incident report templates.** It does bear repeating that the atmosphere among colleagues under pressure responding to a material incident can be very intense. Hence, rather than pulling up a blank reporting template and filling it in from scratch, an organization should have access to templates that have already been pre-populated ahead of time with a subset of the basic information required. The details of the specific incident itself can then be added in real time. As far as possible, incident reporting templates should use the same or similar formats across different agencies to reduce the administrative burden. Lobbying for that should form part of the initial engagement in the consultation process when new proposals are first published. ■

About the Sponsors

The sponsors of this White Paper are Cyber Threat Alliance and Palo Alto Networks. Details of both organizations follow below.

About Cyber Threat Alliance

The Cyber Threat Alliance (CTA) is a 501(c)(6) non-profit organization that is working to improve the cybersecurity of our global digital ecosystem by enabling near real-time, high-quality cyber threat information sharing among companies and organizations in the cybersecurity field. We take a three-pronged approach to this mission:

1. Protect End-Users: Our automated platform empowers members to share, validate, and deploy actionable threat intelligence to their customers in near-real time.

2. Disrupt Malicious Actors: We share threat intelligence to reduce the effectiveness of malicious actors' tools and infrastructure.

3. Elevate Overall Security: We share intelligence to improve our members' abilities to respond to cyber incidents and increase end-user's resilience.

CTA is continuing to grow on a global basis, enriching both the quantity and quality of the information that is being shared amongst its membership. CTA is actively recruiting additional cybersecurity providers to enhance our information sharing and operational collaboration to enable a more secure future for all. For more information about the Cyber Threat Alliance, please visit www.cyberthreatalliance.org

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com

Palo Alto Networks Unit 42 brings together world-renowned threat researchers, elite incident responders, and expert security consultants to create an intelligence-driven, response-ready organization that's passionate about helping you proactively manage cyber risk. Together, our team serves as your trusted advisor to help assess and test your security controls against the right threats, transform your security strategy with a threat-informed approach, and respond to incidents in record time so that you get back to business faster. For more information visit www.paloaltonetworks.com/unit42.

About HardenStance

HardenStance provides trusted research, analysis and insight in IT and telecom security. HardenStance is a well-known voice in telecom and enterprise security, a leader in custom cyber security research, and a leading publisher of cyber security reports and White Papers. HardenStance is also a strong advocate of industry collaboration in cyber security. HardenStance openly supports the work of key industry associations, organizations and SDOs including NetSecOPEN, AMTSO, OASIS, MEF, The GSMA and ETSI. HardenStance is also a recognized Cyber Threat Alliance 'Champion'. To learn more visit www.hardenstance.com

HardenStance Disclaimer

HardenStance Ltd has used its best efforts in collecting and preparing this report. HardenStance Ltd does not warrant the accuracy, completeness, currentness, noninfringement, merchantability or fitness for a particular purpose of any material covered by this report.

HardenStance Ltd shall not be liable for losses or injury caused in whole or part by HardenStance Ltd's negligence or by contingencies beyond HardenStance Ltd's control in compiling, preparing or disseminating this report, or for any decision made or action taken by user of this report in reliance on such information, or for any consequential, special, indirect or similar damages (including lost profits), even if HardenStance Ltd was advised of the possibility of the same.

The user of this report agrees that there is zero liability of HardenStance Ltd and its employees arising out of any kind of legal claim (whether in contract, tort or otherwise) arising in relation to the contents of this report.