HERBERT SMITH FREEHILLS

ARE YOU PREPARED? THE BOARD'S ROLE IN CRISIS MANAGEMENT

10 October 2019 | Global
Legal Briefings – By **Joseph Falcone, Katherine Gregor, Julian Lincoln, Andrew Moir, Andrew Procter, Mark Robinson and Kate Macmillan**

With the ever-increasing growth in the number and potential magnitude of cyber, technological and operational risks to financial services entities, boards need to be prepared to respond to these types of crisis and ensure that the entity's critical information assets are appropriately secured.

The role of a board, in particular the non-executive members, changes dramatically in a time of crisis. Customers, the public, regulators, and policymakers expect the board to steer the firm confidently and competently back to safety.

While it is fair to say that a board should consider and plan in advance for how to respond to a crisis, there is a balance to be struck. A board should not be structured solely with crisis management in mind, given that crises are likely to be quite rare. However, the prominence that a board is likely to have during a crisis means that it is sensible to consider the collective crisis management skillset. The Chair (and/or in the case of large firms, the Nominations Committee) should regard this aspect of the board's functions when considering potential new appointments and when commissioning a Board Effectiveness Review.

REGULATORY OBLIGATIONS FOR BOARD MEMBERS

Boards of financial services entities need to have clear systems and strategies in place to manage the security of data and information assets and respond to incidents, as this is fundamental to the stability of both their business as well as the broader financial markets. The operation and reputation of a financial services entity depends on the security and resilience of its technology systems and regulators around the world are sharpening their focus on technology, operational and non-financial risks.

For example, in Australia, the Australian Prudential Regulatory Authority (**APRA**) has recently issued Prudential Standard CPS 234 (**CPS 234**) which makes the board of an APRA-regulated entity ultimately responsible for ensuring the entity maintains its information security. This means that the information security related roles and responsibilities of the board and senior management need to be clearly defined and the board must ensure the entity has controls to protect its information assets and undertakes systematic testing and assurance around the controls effectiveness. APRA's latest Corporate Plan also names improving cyber resilience across the financial system as one of its top four strategic focus areas.

In the United States similar obligations are placed on the board. One example is the "Cybersecurity Requirements for Financial Services Companies" issued by the New York State Department of Financial Services (**DFS**) in 2017 (**Regulations**), which has implementation and compliance deadlines through 2019. These Regulations require each covered entity to assess its specific risk profile and establish and maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of its information systems. These Regulations apply to any individual or non-governmental entity (unless exempt), operating or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorisation under the New York Banking Law, Insurance Law, or Financial Services Law.

> **The Regulations "require the establishment of governance processes to ensure senior attention to these important protections".**
> **"Senior management must take this issue seriously and be responsible for the organisation's cybersecurity program and file an annual certification confirming compliance with these regulations" including "a written policy or policies that are approved by the Board of Directors or a Senior Officer."**
> ***DFS Superintendent Maria T. Vullo, December 2018***

In Europe, we find clear expectations for boards or "Management Bodies" in the EU Capital Requirements Directive IV (**CRD IV**), in addition to the provisions of the Companies Act and the non-binding Financial Reporting Council's Corporate Governance Code. The legislation sets out the expectation that board members should commit sufficient time to perform their functions and sets restrictions on the number of additional directorships an individual board member may hold. CRD IV and the provisions of the second Markets in Financial Instruments Directive (**MiFID II**) are further bolstered with guidance from the European Banking Authority (**EBA**) and the European Securities and Markets Authority (**ESMA**).

The financial crisis of 2007/8 has seen policymakers and regulators become increasingly focused on ensuring that the boards of financial institutions are robust and fit for purpose–including managing a crisis. The focus on time is important as steering a firm through a crisis, from inception to the post-crisis tail, will take a significant time commitment: dealing with a cyber event, such as a large personal data breach impacting upon multiple stakeholders or the unavailability of a critical IT system, can become a full time job in the months following the incident.

LITIGATION AND PERSONAL LIABILITY

Litigation following cyber incidents will often argue that executive directors should be personally liable on the basis of breach of fiduciary duty. Irrespective of the law, executive board members have frequently stood down from leadership roles following significant data breaches.

> **"CEOs and other decision makers should be held accountable whenever a cybersecurity breach takes place"…"Organisations need to see cyber attacks as a business risk and leadership at the highest levels have to take accountability."**
> ***Mr David Koh, Chief Executive of the Cybersecurity Agency of Singapore (CSA), September 2018***

In the UK, some in a non-executive capacity might be uneasy about whether they have met their obligations to the firm under the FCA's Senior Managers and Certification Regime (**SMCR**) (see Financial Conduct Authority Handbook, Code of Conduct, Annex 1/1, Roles and Responsibilities of NEDS of SMCR firms), such as the role of satisfying themselves that systems of risk management are robust and defensible. However, while there is a temptation to move into a more executive mode, the fact they may have a greater degree of distance from the fray can enable them to take a more measured stance representing the firm externally.

PREPARING THE BOARD FOR A CYBER INCIDENT

In 2018 the UK Government's Cyber Governance Health Check, which looks at the approach the UK's FTSE 350 take to cyber, concluded that many FTSE 350 boards still do not understand the impact of a cyber incident on their business. Similarly, the UK FCA's cyber and technology resilience survey (November, 2018) highlighted that firms reported a lack of board understanding of cyber risks, an issue which the FCA has also seen during its supervisory work. In Australia, capabilities across APRA's regulated entities and their key service providers are variable with a range of cyber exposures and preparedness observed by the regulator.

In order to counteract the lack of cyber understanding prevalent at board level, we are seeing a number of strategies being implemented such as establishing specialist sub-committees and conducting simulation or "Wargaming" activities. In particular, when modelling simulation scenarios for cyber incidents, attention should be given to containment and mitigation strategies.

CRISIS SIMULATIONS

It is common practice for firms to engage in crisis management simulations–a task which is not to be underestimated given the need for policies, plans, and procedures to be comprehensive and flexible to cover any combination of circumstances. It is important for boards to be fully engaged with the firm's crisis management simulations and to understand the firm’s activities and main risks. For example, in the EU, CRD IV requires firms to devote adequate resources to induction and training of board members to ensure they possess adequate collective knowledge, skills, and experience.

In the case of a cyber or broader technology incident, adequate simulation training may ensure there is appropriate capability within the board to strategically assess and manage the risks upon briefing from an IT Director or Chief Information Security Officer, allowing for a strategic quick response in a time sensitive situation. Such crisis simulations are also important because they acclimatise boards to the sorts of decisions they will need to make in a real incident.

Such “wargaming" is also useful because it can contribute to meeting the "training" expectations of legislation, in which simulation scenarios are carefully constructed to undertake a test of the board's role and response in a crisis situation. Such exercises are likely to be most effective when the board sets aside a reasonable amount of time to fully engage with the exercise, review the outcomes and identify any gaps, for example, at a board away-day or offsite. Without wargaming it is unlikely that the board will be able to meet the very tight timetables that are set for reporting by law.

Reporting requirements – how long have you got?

	Within 1 hour	Within 72 hours	Within 10 business days
UK		Under the General Data Protection Regulation (GDPR), an organisation must report a personal data breach, which is likely to result in a risk to a person's rights and freedoms, to the relevant Supervisory Authority.[1] If the breach represents a high risk to a person's rights and freedoms, the organisation will also have to inform people affected "without undue delay".	
Australia		CPS 234 requires an APRA-regulated entity to notify APRA as soon as possible and in any event within no later than 72 hours after becoming aware of an information security incident that affects or could have materially affected the entity or the interests of customers, or has been notified to other regulators (either in Australia or other jurisdictions);	CPS 234 requires an APRA-regulated entity to notify APRA as soon as possible and in any event within no later than 10 business days after it becomes aware of a material information security control weakness which the entity expects it will not be able to remediate in a timely manner.
Singapore	The Monetary Authority of Singapore (MAS) imposes stringent technology risk management and reporting requirements on financial institutions, such as the requirement to notify MAS within one hour of discovering a system malfunction or IT security incident that has severe and widespread impact on the financial institution's operations or materially impacts on its service to its customers.	Singapore's Personal Data Protection Commission of Singapore (PDPC) requires organisations to report personal data breaches "as soon as practicable" and in any event no later than 72 hours after establishing that the data breach is likely to result in significant harm to be affected individuals or if the breach is of significant scale.	
US		Under the Cybersecurity Requirements for Financial Services Companies referenced above, the covered entity must notify the DFS of any breaches as promptly as possible but no later than 72 hours from a determination that any act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt, or misuse an information system or information stored thereon, has occurred, if: (1) notice is required to be provided to any government body, self-regulatory agency or any other supervisory body; or (2) the event has a reasonable likelihood of materially harming any material part of the normal operation(s) of the entity.	

1. The clock starts ticking from the time when a controller "becomes aware" of a personal data breach, which means when a controller has a "reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised." The rationale for the notification is so that prompt steps can be taken to mitigate any harm which may be caused.

PREPARING A CRISIS RESPONSE PLAN

All organisations should have robust, well-tested incident response plan ready to launch when cybersecurity or technology incidents arise. The key parts of this plan are likely to involve crisis organisation, information and reporting, communications, legal fallout and the aftermath.

ONLY 57%

TESTED INCIDENT PLANS REGULARLY

ALTHOUGH MOST COMPANIES HAD INCIDENT PLANS, ONLY 57% TESTED THEM ON A REGULAR BASIS. BUSINESSES IN FINANCIAL SERVICES WERE AHEAD OF THE PACK, HOWEVER, AS THEY WERE SLIGHTLY MORE LIKELY TO TEST THEIR PLAN REGULARLY, WITH 61% DOING SO, COMPARED TO 49% IN OTHER SECTORS.

THE UK GOVERNMENT'S CYBER GOVERNANCE HEALTH CHECK

CRISIS ORGANISATION

There is a balance to be struck between being comprehensive and being flexible to suit any combination of circumstances. If the plan is too rigid, then adhering to it becomes impractical and, in the worst case scenario, serves to exacerbate the crisis. If the plan is too high level, it offers little guidance at a time when that is likely to be needed. The best plans include the detail, but indexed and cross-reference in a way that is easily navigable for any given type of incident.

In a board context, it is important that – at time of crisis – the respective roles and responsibilities of the various board members are clear and take into account the relevant skill sets.

Typically, the chair of the board will have a leading role in a crisis. However, there may be types of crises where a board member's profile or skill set is particularly suited for a lead role – for example, if a board member has considerable and relevant reputational capital or technical skills. The plan should allow for the chair to make delegations where appropriate and beneficial for the firm.

The plan should also be clear on the respective roles of the executive versus the non-executive, particularly with regard to representing the firm externally. Given the direct management role which the executive plays in the day-to-day running of the firm, there is potential for those in executive roles to become defensive during a crisis. This is particularly true where external parties – for example, politicians, the media, social media commentators – allude that there may be a degree of personal culpability attached to an individual executive.

INFORMATION AND REPORTING

Many crises require the rapid collation of information from different teams. Cyber crises, for example, require input at speed from many different disciplines, including technical, legal, business continuity and communications – and, given the international nature of many cyber incidents, often across a number of jurisdictions. It is often advisable to appoint a dedicated coordination team to ensure that information is collated sufficiently quickly.

In cyber incidents one of the first steps may be to engage alternative means of communication, given that there may be lack of clarity regarding which systems have been impacted. For example, if corporate e-mail is compromised, it may be necessary to resort to alternatives such as WhatsApp. It is too late to try to set such alternative communications up after the event; it must be done beforehand and be part of the crisis response plan.

While the management information which a board will receive to inform its business-as-usual oversight typically evolves to suit the needs of the board over time, during a crisis there is not time to finesse its formatting and content. An exercise should help to build the board's awareness of and (potentially) familiarity with management information in formats, structures, and volumes which they would be unlikely to use during business-as-usual periods.

During the investigation, care should be taken to log investigative steps and to preserve evidence in case civil or criminal proceedings follow.

LEGAL FALLOUT

The role of legal in any incident can be significant. The legal team's input is often required to help contain the incident, to manage regulatory, insurance and other notifications, to manage third parties that may have had a hand in the incident (for example, a third party supplier), to manage any subsequent investigation and to deal with any follow-on claims. Much preparation can be done in advance, and it is common for legal teams to have their own, separate legal incident response plans in order to accelerate their ability to respond in a crisis.

As part of this, the plan should provide for careful consideration of what documents might attract legal professional privilege and how that privilege can be best preserved throughout the incident and subsequent investigation – bearing in mind that there will often be a trade-off between preserving privilege and stifling efficient and important communications during a crisis.

EXTERNAL COMMUNICATIONS

Crises have the potential to throw firms into disarray and it is critical to manage external messaging, particularly where social media has the ability to proliferate both real accounts and "fake news". Great care should be taken by board members and it is common practice to provide media training as part of the simulation exercises; such as role playing with specialist media consultants. The challenge is to avoid saying anything that may prove to be a hostage to fortune, while also meeting regulatory expectations to keep stakeholders, including customers, informed.

Where possible, the board should consider what steps a firm might take around communications in the crisis plan, eg heightened monitoring of media and social media, the prioritisation of particular channels and/or the general tone/positioning of external communications; the slightest misstep may be seized upon and spun via mainstream or social media. This could lead to loss of customer trust, with significant reputational and financial consequences.

Responsibility for both approval and delivery of external messaging should also be part of the role allocation process, with consideration given to the audience eg staff, shareholders, the mainstream media, social media, government and politicians, regulators, peer firms, and the wider industry. Consideration should also be given to the timing and rhythm of communications as the crisis develops, so that key stakeholders are notified simultaneously regarding developments, and that there is consistency to the narrative as the crisis unfolds. In cyber incidents it can take time to determine what has happened; to identify correctly the threat actor and their motivation.

For instance, when an airline operator suffered a large-scale data breach in 2018 with 9.4 million of its passengers impacted, the airline was heavily criticised by the Hong Kong Privacy Commissioner for taking seven months to disclose its breach and not having enough regard for data privacy and governance. Unlike the GDPR's requirement to disclose data breaches within 72 hours, Hong Kong currently has no statutory requirements for data breach notifications. Nevertheless, the privacy watchdog has stated that businesses should adopt "proactive data management " despite Hong Kong not having "a similar principle of accountability" as the EU.

Some of the messages which a firm conveys are subject to regulatory or legal requirements. For example in the UK, firms are expected to disclose anything of which the regulators would reasonably expect notice and for the firm to keep customers appropriately informed. While quite a broad-ranging requirement, a crisis would certainly fall within the disclosure expectations. Similar requirements may emanate from other authorities, for example, those charged with upholding data protection standards like the UK's Information Commissioner.

It is crucial to dovetail any external public communications with regulatory, insurance and other notifications, to avoid regulators finding out about incidents via the press rather than from the firm directly.

CRISIS AFTERMATH

Crisis events can, and usually do, have a very long tail – often extending years after the event. Plans which are circumscribed to the immediate aftermath of an incident risks validating a short-sighted approach. While a firm cannot, and should not, run in crisis mode for longer than is reasonably needed, the "exit" or "close out" should include a sensible "lessons learned" exercise, including updating the crisis plan, to meet the expectations of customers, the public, regulators and policymakers.

The board should consider any impacts on, for example, the firm's risk appetite and governance arrangements, customers and potential customers, the regulatory relationship, and so on. In a recent enforcement action against a UK bank which related to an IT failure, the UK regulators highlighted that the firm had previously been subject to enforcement action for a similar incident. Commenting on the case, the CEO of the Prudential Regulation Authority noted, "… this was a repeat failing which demonstrates a lack of adequate and timely remediation. This is a significant aggravating factor in this case, leading to an uplift in the penalty." While not known for sure, it may also be reasonably conjectured that the regulators' supervision of the firm will have become more intensive.

CONCLUSION

While it is not possible to plan for every eventuality, boards have a key leadership role in preparing their firms to respond effectively to and recover from a crisis.

As society becomes increasingly digital and data-driven, the harm that can be caused by a cyber incident has become greater. Accordingly, the expectations of board members by regulators, stakeholders and the public are higher than they have ever been. Increasingly, boards will be expected to understand the technologies better that are being widely deployed in business. They will be expected to keep up with the changing threat landscape and oversee the implementation of security controls which are appropriate for the new landscape. The consequences of not meeting those expectations are severe.

Digital transformation and developments in, for example, blockchain-based technologies, machine learning/artificial intelligence and quantum computing will bring further rapid, substantial change. In the future, board members will be assisted by security being built into new products and services by design and default to a greater extent. For now, however, risk-based planning, including a well thought through and robustly tested incident response playbook, that is proportionate to the scale and complexity of a firm's operations will do much to minimise operational damage, reputational harm and legal liability. Preparations do not have to be onerous, and should, in the best cases, provide the board with more insight into the business to improve how they function during business-as-usual.

Read more in our 2019 Global Bank Review: The Data Game

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

ANDREW MOIR
PARTNER, INTELLECTUAL PROPERTY AND GLOBAL HEAD OF CYBER & DATA SECURITY, LONDON
+44 20 7466 2773
Andrew.Moir@hsf.com

KATHERINE GREGOR
PARTNER, MELBOURNE
+61 3 9288 1663
Katherine.Gregor@hsf.com

MARK ROBINSON
PARTNER, SINGAPORE
+65 68689808
Mark.Robinson@hsf.com

ANDREW PROCTER
PARTNER, LONDON
+44 20 7466 7560
Andrew.Procter@hsf.com

JOSEPH FALCONE
PARTNER, NEW YORK
+1 917 542 7805
Joseph.Falcone@hsf.com

JULIAN LINCOLN
PARTNER, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

KATE MACMILLAN
CONSULTANT, LONDON
+44 20 7466 3737
kate.macmillan@hsf.com

LEGAL NOTICE