Transparency in the digital age: companies should talk about their cyber security

pwc

The cyber security of companies is an increasingly important issue for society.

Nations depend on the cyber security of both public and private institutions for them to function, with critical infrastructure and even our democracies increasingly targeted by cyber attackers.

For companies, successful cyber attacks could result in material fines, legal actions, operational outages, and adverse impact on stakeholders. Individuals need to be confident that vast amounts of personal data submitted to organisations is safe and that the digital services on which they increasingly depend are reliable. And as rapidly more connected devices enter our personal world, our safety is even at stake.

Yet most companies are not reporting anything meaningful of their efforts to mitigate the threat. Shareholders, the public and other stakeholders deserve better: it is time to think seriously about more effective corporate reporting on cyber security.

Reporting on cyber security is thin on the ground – that needs to change

The reluctance of companies to report insightfully on cyber security is at first sight understandable. Companies may be concerned that reporting would increase their vulnerability to attack if they were to make public information that is useful to attackers. Or they may be anxious about revealing shortcomings that could leave them open to legal or regulatory scrutiny, particularly where they do not have a comprehensive global view of all the regimes with which they must comply.

There are links to more general concerns about the value of reporting. Boilerplate style reporting on cyber security will provide little insight into how a company is specifically managing its cyber security risk. Similarly, over-reporting is not helpful; setting out all possible risks but providing no information of value on how they are being managed. Truly meaningful reporting on cyber security will flow from a considered view of its relevance to a company's business model and strategy.

However, responsible and accountable companies need to confront these challenges. Businesses themselves accept that building strong cyber security is of fundamental importance to their future prospects; PwC's recent CEO research[1] reveals that boards see cyber attacks as the most rapidly developing threat they face. Failure to report on efforts to counter the threat is not sustainable.

Investors' concern over cyber security risk is increasing. Recent PwC research[2] shows investors now regard cyber attacks as the biggest threat to the companies in which they have shareholdings. Other stakeholders also need reassurance. Customers are losing faith in the ability of companies to safeguard their personal information and protect them from attack: PwC research[3] in the US published last year found just 25% of consumers think most companies handle their sensitive personal data responsibly. Companies will need to work harder to establish trust and reporting has a role to play.

Moreover, those companies not yet ready to satisfy this demand for more meaningful cyber security reporting may soon find themselves forced to take action. Cyber security and data privacy are rising up the regulatory agenda, not least courtesy of the European Union's General Data Protection Regulation (GDPR). In the UK, the Financial Reporting Council[4] urged companies to improve reporting on cyber security as early as 2016.

Cyber security reporting is also relevant to the governance reform debate in the UK in the wake of recent corporate failures. This has led to a revised UK Corporate Governance Code that puts more onus on businesses to consider their impact on society; cyber security is without doubt a major part of this.

In the US, meanwhile, the Securities and Exchange Commission is increasing its scrutiny of how companies report on cyber security. In February 2018, it set out new guidance[5] to public companies on how it expects them to prepare disclosure about cyber security risks and incidents. This guidance includes a warning that the SEC regards a material breach as market sensitive information.

So, while companies may be forgiven for feeling nervous about reporting in more detail on cyber security, it will increasingly be expected and omissions noted. There is a growing understanding that society now expects a higher level of accountability[6] from businesses. CEOs and their boards have a responsibility to provide greater insight and transparency as to how they are managing what they perceive to be one of the most dangerous threats to their businesses – key stakeholders are keen to hear more and regulators will increasingly require better disclosure.

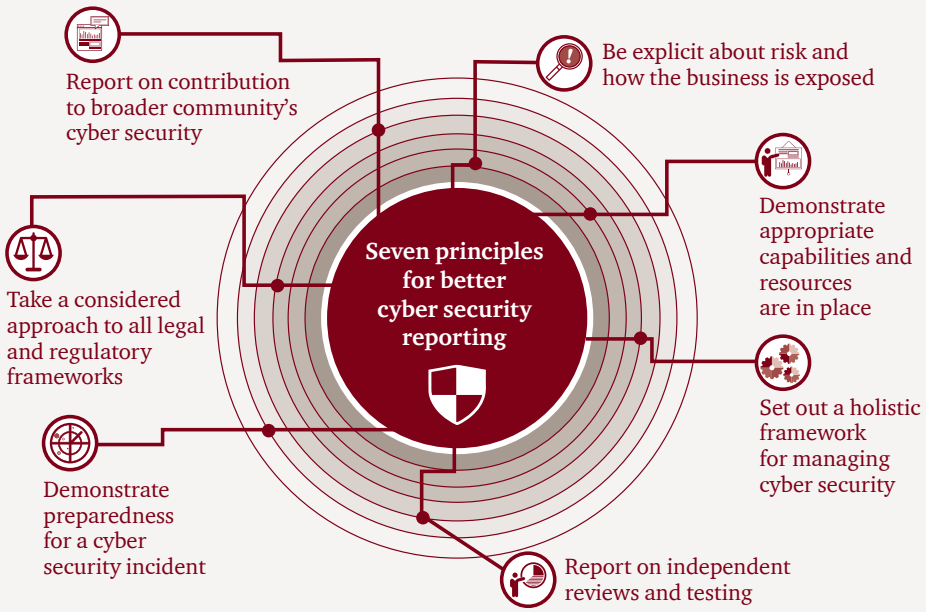
1 https://www.pwc.com/gx/en/ceo-agenda/ceosurvey/2018/gx/business-threats.html
2 https://www.pwc.com/investorsurvey
3 https://www.pwc.com/us/en/services/consulting/library/consumer-intelligence-series/cybersecurity-protect-me.html
4 https://www.frc.org.uk/getattachment/4033d078-55b7-415d-922a-e25ea0070376/Annual-Review-of-Corporate-reporting-2015-16-FINAL.pdf
5 https://www.sec.gov/rules/interp/2018/33-10459.pdf
6 https://www.pwc.co.uk/services/audit-assurance/insights/ftse-350-reporting-trends-.html

What can and should companies do?
Seven principles for better cyber security reporting

No company can reasonably be expected to set out the detail of their cyber security defences – to do so would be to declare their hand to would-be attackers, or even be regarded as a challenge.

However, it is possible for companies to make meaningful disclosures about their cyber security policies and practices without falling into the traps that worry many companies. In doing so, companies have an opportunity not only to provide crucial reassurance to key stakeholders – and to meet their regulatory duties – but also to play a constructive role in building a more secure digital society.

To achieve this, companies could and should report in detail on their cyber security governance: what structures and capability have been put in place to manage the risk. Below, we set out principles that we believe companies should adopt for cyber security reporting. These principles reflect our views[7] about how boards should consider the governance of their organisations' cyber security endeavours. This is where we see the greatest opportunity for value additive reporting.



1. Be explicit about the risk and how the business is exposed

The basis for cyber security governance has to be a full understanding of the extent to which a company is exposed to cyber risk, and how it is material to their business model and strategy. Companies should explicitly detail the risks they have identified and the potential impacts of cyber breaches – not just to themselves, but to other organisations and wider society should their defences be breached. They should specify what data and processes might be targeted and why, and the ways in which attacks might materialise, including through their supply chain.

The objective here is to report on the extent to which the company and its senior executives clearly understand the evolving threat posed by cyber security and how that threat could impact both the company and others. It also enables stakeholders to grasp the extent of the inherent risk the company faces.

2. Demonstrate that appropriate capabilities and resources are in place

More granular reporting on capability would include detail such as who, at executive committee level, is ultimately responsible for cyber security. It could also identify key operational executives such as the chief information security officer (CISO), their background and experience for the role and the size of the security function they lead.

Companies should report on the adequacy of the board's oversight, including: relevant expertise of board members; and how much time the board devotes to discussion of cyber security-related issues, whether at full board level or in committee, and what these discussions cover. One important question will be how the board establishes that resourcing throughout the company is adequate and appropriate.

Finally, it would be useful to provide some measure of how engaged the organisation as a whole is on cyber security issues – the extent to which all staff are risk aware and conscious of the precautions they should take.

7 https://www.pwc.co.uk/issues/cyber-security-data-privacy/insights/governing-cyber-security-risk.html

3. Set out a holistic framework for managing cyber security

Good reporting will include detail of how the company structures its controls and its broader approach to cyber security risk management. One element of this reporting will be to state whether the company operates according to a recognised framework, such as those published by the US National Institute of Standards and Technology (NIST). While these are a helpful way to define what cyber security controls are in place, companies should also be able to report on their broader processes and culture. For example, how is the question of cyber security hardwired into decision making processes throughout the company?

A company should also be able to report on how it measures its cyber security effectiveness – what metrics are in place and how risk appetite converts into quantitative measures.

4. Report on independent reviews and testing

All boards should commission regular independent reviews and testing of their companies' cyber security controls and effectiveness. There is no reason why companies should not report on such reviews, including the frequency of independent reporting to the board, credentials of the reviewer and scope of the reviews. The extent to which third party testing has been carried out through realistic ethical hacking should also be included in this reporting.

Companies will not want to publish detailed findings of reviews and tests, given that these will include details of vulnerabilities. But they should be able to report on the time devoted by the board to discussing independent reviews, as well as the extent to which recommended actions have been implemented.

Finally, new formal attestation approaches are coming to market such as the 'SOC for Cybersecurity' framework from the American Institute of Certified Public Accountants (AICPA) which may enable more granular reporting on cyber security controls and processes, validated by a third party.

5. Demonstrate preparedness for a cyber security incident

Companies should not feel uncomfortable reporting that they have thought in detail about how they would respond in the event of a significant cyber security incident. No company can ever be confident their defences will repel all attacks, and preparedness for a major breach is critical.

Reporting in this area can be detailed without giving away sensitive information. Companies should be able to demonstrate they have plans in place for containing any breach; ensuring appropriate disclosure; restoring business as usual, and investigating the incident. They should also be able to report on broader crisis management readiness, such as how they will communicate with those affected by an incident; how regularly they exercise their crisis management capability; and extent of insurance cover in place for a cyber breach.

In addition, disclosure of incidents that have occurred during the reporting period should be a key tenet of transparency. While companies are increasingly legally required to report significant incidents and breaches as they occur, they should set out the total number and nature of incidents they have dealt with over a given period, including smaller incidents not previously disclosed. It should also be possible to report on the lessons learned from such incidents, as well as the speed with which the company detected and responded to the incidents.

This may feel uncomfortable. But the reality is that, as cyber security reporting matures, companies not reporting they have suffered an incident should be a cause for concern for key stakeholders. Such companies would either be failing to report or, more alarmingly, missing such incidents in the first place, even though they have almost certainly taken place.

6. Provide confidence that a considered approach is taken to all relevant legal and regulatory frameworks

Companies should report on the legal and regulatory regimes with which they are required to comply. Some of these regimes are likely to be near universal: the GDPR, for example, has extensive reach. Others may only be relevant to companies operating in particular geographies or industries. Relevant law and regulation will include both regimes governing cyber security practices and those that set out requirements for cyber security reporting itself.

It is important that boards establish their recognition and understanding of the regimes that apply to their businesses. Reporting should include disclosure of any legal or regulatory breaches that have occurred, with detail on the consequences, as well as information on how the company is meeting its statutory responsibilities moving forward.

7. Report on contribution to the broader community's cyber security

No company can defend itself in isolation. Companies should therefore report on how they collaborate with others in their industry, supply chain or customer bases to build a collective defence of their common interests. Participation in information sharing schemes and joint funding of defence initiatives are examples of measures that could be reported. In addition, companies should report on how they collaborate with law enforcement and national cyber security agencies.

This reporting should demonstrate directors' understanding of the importance of collaboration to bolster cyber security - as well as their awareness of their broader societal duties. Such disclosures are likely to become more important as stakeholders such as customers look to businesses to do more to protect them.

The legal burden in this area is also getting more focus. For example, Section 172 of the UK Companies Act 2006 requires companies to explain how directors have had regard to the interests of employees, the relationships with customers and suppliers, the impact on the community and the desire to maintain a reputation for high standards of business conduct. This will increasingly require consideration of cyber security.

Checklist for Cyber Security Reporting

1. Real understanding of exposure

- Explicit description of key areas of risk:
  - what might be targeted and why
  - how the company might be attacked indirectly through dependencies on others
  - how a cyber breach might impact stakeholders

2. Appropriate capability and resource

- Named executive accountable for cyber security
- Name and experience of the cyber security leader (CISO)
- Size, structure and reporting line(s) of security function
- Capability/experience of Non-Executive Directors
- Board time (including in committee) devoted to cyber security and topics covered
- Approach to ensuring adequate resource is dedicated to cyber security

3. Holistic framework and approach

- Recognised framework(s) followed (eg NIST)
- Governance mechanisms to ensure cyber security is 'baked into' key decision making
- Staff engagement
- Measures and metrics adopted

4. Independent review and test

- Approach to independent review, scope of reviews, qualification of reviewer(s) and rationale for appointment
- Approach to testing of controls (eg simulated attacks by ethical hackers, 'SOC for cybersecurity' reports)
- Board commitment to implementing recommendations

5. Incident preparedness and track record

- Approach to ensuring organisation is prepared to respond to major breaches
- Insurance coverage for cyber breaches
- Evidence of exercising
- Reporting of both major and minor incidents, lessons learnt, speed of detection & response

6. Considered approach to legal and regulatory environment

- Description of key regulatory and legal requirements for cyber security in all relevant jurisdictions
- Description of any legal or regulatory breaches

7. Community contribution

- Approach to collaboration with others in industry, through supply chain and with dependent customers
- Approach to collaboration with law enforcement and national cyber security agencies in key territories

Conclusion

The cyber security of our public and private institutions is growing rapidly as a significant issue for society. Greater transparency as to how organisations manage cyber security risk is an imperative and companies need to respond. Corporate reporting of cyber security risk management will doubtless develop as the digital world in which we live evolves; the challenge for all companies now is to begin the journey to provide meaningful insight into how they manage the risk. The approach outlined in this paper can provide a structure to enable them to take the critical first step.

About the Author

Dr Richard Horne is a specialist partner in PwC UK for cyber security, advising boards of global and national organisations on the subject. A recognised authority and press commentator on cyber security, he is also a board advisor to a number of early-stage cyber security companies. Prior to joining PwC, he led cyber security for a global universal bank, and was seconded to the UK government to help shape the national plan for cyber security.

Richard can be contacted at richard.horne@pwc.com, and would be delighted to receive comment or suggestions to improve and develop the thinking in this paper.

About PwC

With offices in 157 countries and more than 223,000 people, PwC is among the leading professional services networks in the world. We help organisations and individuals create the value they're looking for.

Our purpose is 'Building trust in society and solving important problems'. In today's digital world that requires a focus on cyber security in order to build a secure digital society. We help clients across society to understand their cyber security risk; build and assure their defences; identify and respond to attacks, and to navigate the complex legal and regulatory environment for cyber security. For more information please visit www.pwc.co.uk/cybersecurity

Design Services 31578 (10/18).