Cyber Resilience

A Priority for Board Members

ICS THE SOCIETY FOR CHARTERED IT PROFESSIONALS IN IRELAND

President's Foreword

Cyber risks affect us all – as individuals and in the organisations where we work. But in organisations, the consequences of a cyber-attack can be far more serious – in terms of the losses suffered, operations paralysed and reputation damaged. For Board Members, the responsibility to address these concerns is enormous and the consequences of not doing so, potentially calamitous.

This Irish Computer Society ("ICS") report highlights key issues arising from a survey of Board Members of Irish organisations, highlighting serious vulnerabilities, including the surprising lack of training of Board Members.

Cyber-security and cyber-awareness are of concern to all of us. We cannot leave it just to the professionals. We must all be aware of the issues and make concerted efforts to improve the security of our systems, our clients and customers, and even our families. This issue will not go away.

There is, however, an upside. We are lucky to have many of the top technology companies with significant operations in Ireland.

I am grateful to Bob Semple and the group of ICS Fellows who have led this initiative, as well as to the organisations and individuals who responded to the surveys and provided us with valuable feedback and results. Many thanks also to the staff of ICS for supporting this activity.

I hope you will find this report to be useful. Perhaps parts of it will make you think just how vulnerable we all are. But this realization gives us an opportunity to change things.

Mike Hinchey
ICS President

"Cyberattacks today are potentially as destructive as major natural disasters.

Too often, businesses find themselves reacting to – rather than preparing for – attacks."

World Economic Forum, July 2020

Contents

The Irish Computer Society

The mission of the Irish Computer Society ("ICS") is to advance, promote and represent the interests of ICT professionals in Ireland.

The ICS works to advance and promote computer literacy throughout the Irish population by:

- Providing a means for current and potential computer users to achieve certified qualifications.
- Encouraging the continuous development and availability of ICT curricula, and the use of appropriate ICT throughout the education system.
- Furthering Ireland's economic, educational and cultural participation in the worldwide Information Society.

1. Introduction

The Irish Computer Society ("ICS") launched this initiative on Cyber Resilience because of:

- the increasing risks from cyber-attacks, and the resulting disruption and cost responding to them,
- the enormous reputational damage that organisations (and individuals) can suffer, and,
- the challenges that Board Members face in addressing these issues.

This report presents the findings of a survey of Board Members of Irish organisations conducted in September/October 2020.
The aim of the report is twofold:

- to help raise awareness among Board Members of Irish organisations of the different types of cyber-attack that their organisations may encounter, and,
- to provide practical guidance on the steps their Boards can take to cultivate greater resilience against those attacks.

The survey results make it clear that urgent action is required in many boardrooms to better equip organisations with the ability to recover rapidly from a cyber-attack. In other words, to improve their Cyber Resilience. Among the most important is raising the capability and confidence of Board Members themselves to provide the necessary direction and oversight.

I hope you find this report stimulating and practical.

Bob Semple
on behalf of the ICS

"85% of directors described cyber risk expertise as very important or somewhat important."

"Only 36% of directors have sufficient director expertise in cyber security."

Annual Corporate Director Survey (USA), PwC, October 2019

"Less than a quarter of new directors [appointed to Irish public companies in 2019] had a digital background . . . and 3 per cent had knowledge of cybersecurity."

Irish Times, 24 September 2020

2. Summary of Findings

Board Members' Comments (Respondents)

"This is a topic that Boards are probably not taking seriously enough."

"I think this is seen as an ICT issue rather than an organisational risk issue."

"I feel potentially quite exposed by lack of knowledge/training in corporate cyber threats."

"The board in general are not computer literate."

These comments, from Board Members who completed the survey, provide an appropriate introduction to the results of the survey.

Answers to the 14 survey questions can usefully be considered under three key headings:

Capability and Confidence

- A significant percentage of Board Members say that they are either not discussing Cyber Resilience at all (21%) or are not being briefed about ongoing developments (32%-44%)
- Four in five Board Members have not participated in any testing of cyber incident response plans in the last year
- One in three say that they have received no cyber training in the last year

Direction and Oversight

- One in six respondents say that their organisation does not have a statement of risk appetite; of those who do, only half are satisfied or very satisfied that it reflects the board's position on Cyber Resilience
- Half of respondents have not been briefed in the last year, or ever, on the threats posed by third party contracts
- Only three in five of respondents are satisfied or very satisfied that people who work in the organisation understand the priority that the board places on Cyber Resilience. Given that most cyber-attacks exploit "human factors", this represents a serious gap in cyber defences
- The results of the survey provide only limited assurance about the adequacy of core cyber defences (identification of assets and the risks threatening them, and implementation of appropriate controls)

Formal Assurance

- Only half of respondents reported having received assurance from management or from independent external testing (about the adequacy of their cyber defences)

Many Board Members will want to study these results before committing to any particular action. We set out below common myths that Board Members will want to guard against in deciding how to respond. Section 3 sets out results in greater detail, which will provide additional insights.

Blueprint for Action

Our purpose in writing this report is to provide a blueprint for Board Members to follow. Section 5 provides 10 top questions to ask, along with 10 suggested Board initiatives (many proposed by respondents themselves).

Myth 1 "The threats are not that serious?"

Cybercrime and cyber warfare are big business. If cybercrime were a country then it would have a GDP equivalent to the 13th largest globally (www.parava.org). The leading practitioners of this black art (typically state-backed) have developed sophisticated approaches that are challenging for even large organisations to counter. The road to dealing with this threat is described well in the "Cyber Kill Chain" (see below), a framework developed by Lockheed Martin for identification and prevention of cyber intrusions activity, especially so-called **'Advanced Persistent Threats'**:

A: Advanced	P: Persistent	T: Threat
Targeted, Coordinated, Purposeful	Month after Month, Year after Year	Person(s) with Intent, Opportunity, and Capability

But you don't have to be a state-backed APT to inflict enormous damage. Some of the biggest losses suffered have resulted from computer viruses, computer worms and other malware, with reported losses ranging from over $1 billion to a staggering $38 billion.

The 10 Most Expensive Cyberattacks of All Time, www.investopedia.com

Myth 2 "Surely, our IT security is strong enough?"

> "There are two types of companies in this world: those that have been hacked and those that don't yet know they've been hacked."
>
> *Dmitri Alperovitch, formerly of McAfee*

Security is usually defined as ensuring an IT system's 'confidentiality, integrity and availability'. Resilience, on the other hand, is 'the capacity to recover quickly from difficulties'.

Traditional cyber security measures are no longer enough to protect organisations from the spate of persistent attacks they are now encountering (see Myth 2). Organisations have realised that, despite their best efforts, sooner or later an attack may get through the best of defences. When this happens, the ability to recover becomes critically important. While cyber security's main aim is to protect data and IT systems, Cyber Resilience focuses more on making sure that the organisation continues to operate, even after attack. The focus is on keeping business goals intact, not just IT systems and data.

Myth 3 "There isn't that much cyber-crime?"

PwC's annual survey of economic crime in Ireland revealed cybercrime to be the most frequently reported type of fraud in 2020, cited by 69% of respondents. The firm noted that this is a particular concern given Ireland's position as Europe's largest data hosting cluster.

According to PwC:

51% of respondents had experienced economic crime in the last 24 months

69% of fraud incidents reported were committed by external perpetrators

13% of respondents report losing more than €5m to fraud over the last 24 months

20% said they did not know how much they had lost to economic crime

https://www.pwc.ie/publications/2020/irish-economic-crime-survey-report.pdf

"The 'NotPetya' Ransomware attack . . . has cost businesses a total of $10 billion and counting, according to White House estimates. The price continues to rise two years after the incident, as insurance claims are litigated."

World Economic Forum, July 2020

Myth 4 "This is Management's job?"

Governance Codes are explicit about the Board's responsibilities:

> "The board should establish procedures to manage risk, oversee the internal control framework, and determine the nature and extent of the principal risks the company is willing to take in order to achieve its long-term strategic objectives."
>
> *FRC, 2018*

> "Advising on key risk is a matter for the Board."
>
> *Code of Practice for Governance of State Bodies, 2016*

Case law makes it clear that while directors are entitled to delegate particular functions to management:

> "The exercise of delegation does not absolve a director from the duty to supervise the discharge of the delegated function."
>
> *re Barings plc, 2001, Chambers Corporate Governance Handbook, 6th edition, p.124*

Myth 5 "I'm not an IT expert – this is not my job?"

Directors' duties (codified in the Companies Act 2014) set a clear expectation:

> "A director of a company shall . . . (g) exercise the care, skill and diligence which would be exercised in the same circumstances by a reasonable person having both – (i**) the knowledge and experience that may reasonably be expected of a person in the same position as the director**; and (ii) the knowledge and experience which the director has."
>
> *CA14, S.228*

The Central bank is unequivocal:

> "There should be a sufficient skill set on the board to challenge and oversee [the cyber security] strategy. This skill set and knowledge should be built upon and refreshed regularly to enable the board to understand the evolving nature of the threat and the implications for the business."
>
> *Thematic Inspection of Cybersecurity Risk Management in Asset Management Firms, Central Bank of Ireland, March 2020*

A Board Member does not need to be a subject matter expert – but (s)he is expected to ask challenging questions.

Myth 6 "We can't afford the measures you're suggesting!"

Large organisations have enormous budgets for addressing cyber risks and Cyber Resilience – and small organisations clearly cannot afford to spend such sums. On the other hand, alert Board Members will know that the exercise of good judgment will guide them towards proportionate responses.

The acid test, surely, must be **"is our response 'reasonable and defensible'?"**

Myth 7 "This is an issue only for big organisations?"

While some cyber criminals target large organisation, many do not discriminate and many types of cyber-attack, for example malicious viruses that just cause damage for the sake of it, have no specific target except to cause mayhem. In targeted cybercrime, criminals often attack the customers and suppliers of organisations rather than the organisation itself. According to one report, 40% of SMEs in Ireland have fallen foul of a cyber-attack leading to theft or loss of company data.

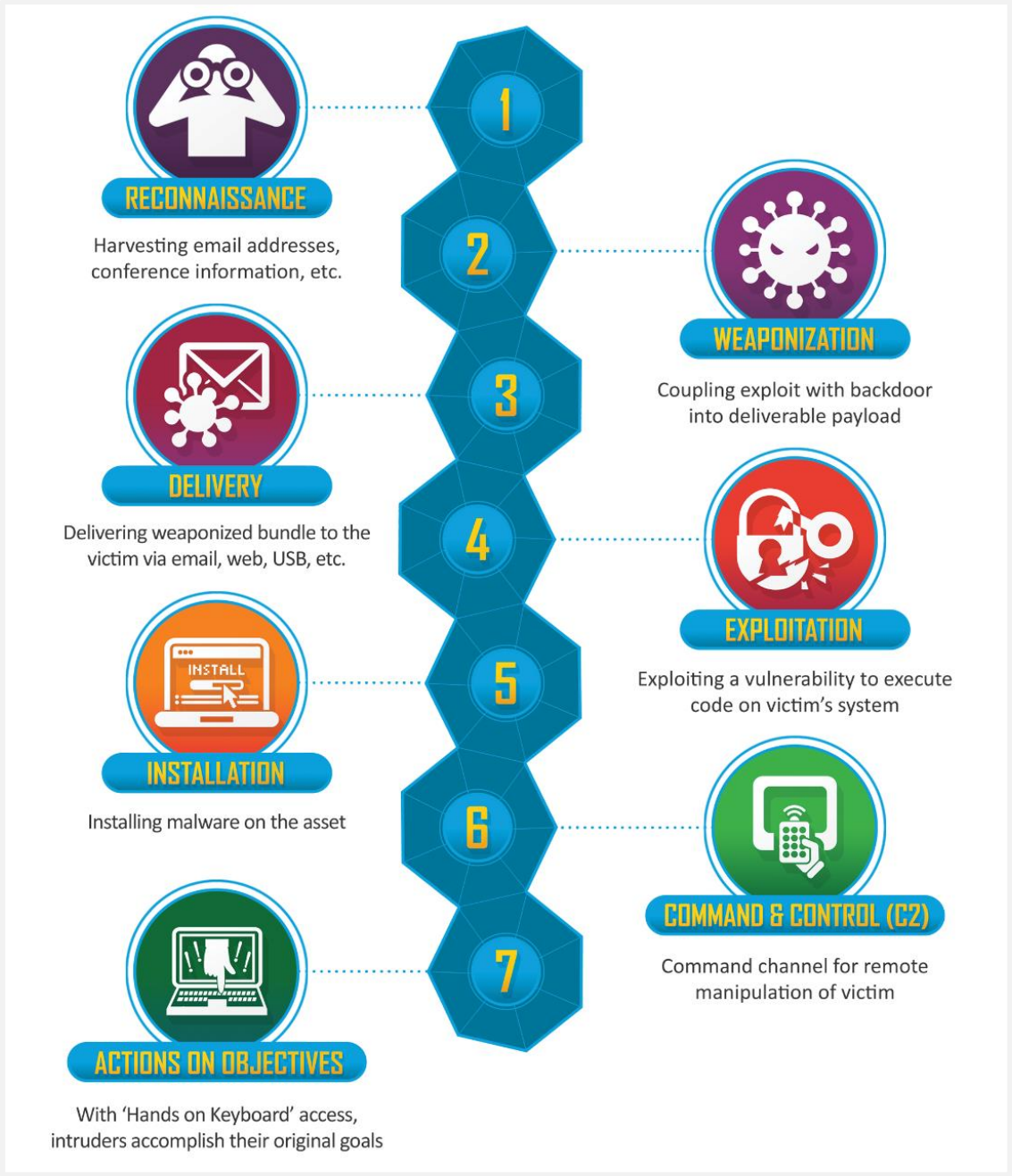
www.irishtechnews.ie, September 2016

The Cyber ‘Kill Chain’

Developed by Lockheed Martin, the Cyber Kill Chain® framework is part of the Intelligence Driven Defense® model for identification and prevention of cyber intrusions activity. The model identifies what the adversaries must complete in order to achieve their objective.

The seven steps of the Cyber Kill Chain® enhance visibility into an attack and enrich an analyst’s understanding of an adversary’s tactics, techniques and procedures.

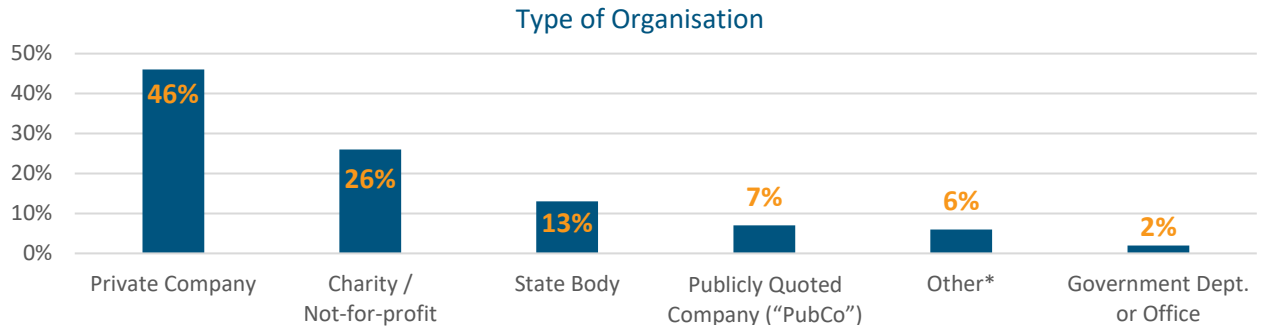
> “Cyber-attacks are a well-run criminal activity. The global cost of cybercrime is estimated in the region of $600Bn.”
>
> *https://www.parava.org/insights/cyber-security-securing-the-corporate-balance-sheet*

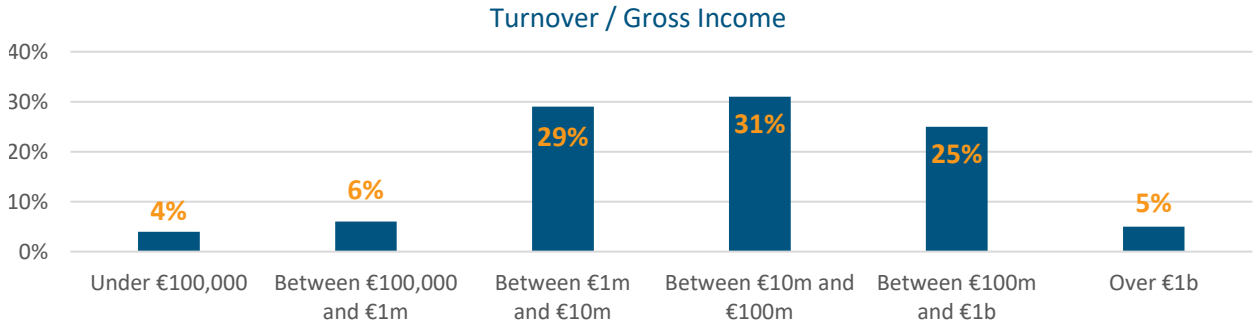


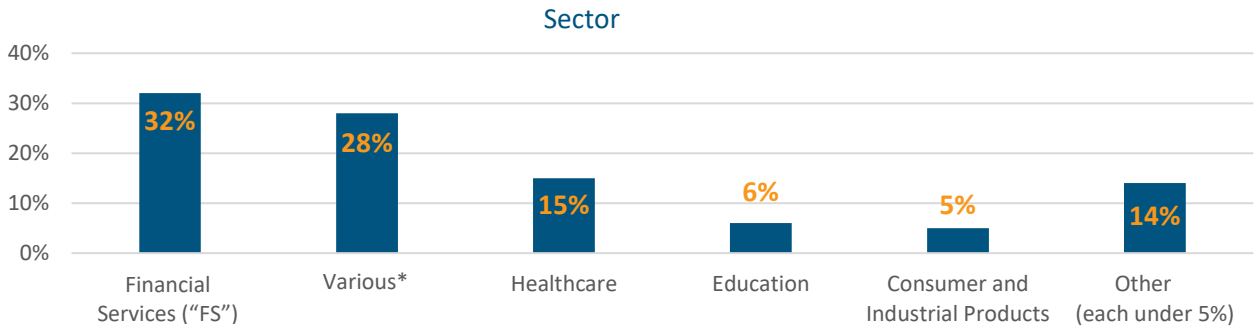
https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

3. Detailed Survey Findings

There were 169 completed responses to the survey, broken down as follows:







* Construction, Public Administration, Energy, ICT, Manufacturing, Real Estate, Utilities

For each of the 3 key areas (described earlier), we set out below:

- A high-level narrative summary
- For each question:

Positive findings revealed by the responses (shown in green) ✓

Areas of concern (shown in red) !

Notable variations from the overall result are shown for types of company, size of Turnover and Sector.

Limitation

Although the level of responses provides worthwhile insights, it is insufficient to provide statistically significant results by subcategory (by sector, by type of company, by size of turnover). Consequently, it would not be valid, for example, to extrapolate the results, say, of the publicly quoted companies included in this survey as representative of all publicly quoted companies. Nevertheless, the results serve a useful role in starting a conversation about what action, if any, needed to be taken to improve the level of Cyber Resilience.

A tabulation of all responses is set out in the Appendix.

Capability and Confidence

High levels of capability and confidence are a prerequisite for any board to effectively interrogate its management. Survey responses to five questions present a troubling assessment:

- one in three received no cyber risk training in the last 12 months
- one in five have not discussed Cyber Resilience at board meetings at all
- only one in five have been briefed on intelligence gathering in the last three months
- one in three have never been briefed on cyber risks arising from third party contracts, and,
- four in five have not participated in any board cyber incident testing within the last year

These results suggest that many boards may be simply unaware of the cyber risks they face, and that training should be put at the top of the list for follow-up action.

Area	Specific findings			
Training (Q5)	34%	**Satisfied or very satisfied with training in last 12 months** *(PubCo: 81%; Cos>€1b: 63%)*	31%	**Received no training in last 12 months** *(FS: 19%; Charities: 58%; Cos<100k: 100%)*
Awareness activities				
• Review of cyber landscape (Q1)	14%	**Have discussed Cyber Resilience as its own topic at every board meeting**	21%	**Have not discussed Cyber Resilience (at all)**
• Intelligence gathering briefing (Q13)	22%	**Briefed on intelligence gathering in the last 3 months** *(PubCo: 50%)*	44%	**Never briefed** *(Charities: 68%; FS: 33%; PubCo: 9%)*
• 3rd party contract exposure (Q11)	51%	**Briefed in last year** *(PubCo: 81%)*	32%	**Never briefed** *(Charities: 66%)*
Board engagement (Q14)	18%	**Participated in a board cyber-incident plan test in last year**	82%	**Participated more than a year ago (9%) or never (73%)** *(PubCo:54%; Cos>€1b:63%; Healthcare: 91%; FS: 67%)*

Board Member Responsibilities – Direction

Survey questions focused on two aspects of 'direction':

- Risk Appetite – Crafting a general statement of risk appetite – formally documenting risks considered acceptable – is one of the more difficult aspects of enterprise risk management. Ensuring that the statement reflects the board's position on cyber risk adds to the difficulty. The survey results suggest that the largest of the companies that responded are best at articulating their risk appetite. However, one in six respondents have no statement of risk appetite at all – which points to the remedial work needed in this area.

- Personnel – Research reveals that the majority of successful cyber-attacks exploit the 'human factor'. As such, Board Members need to place a particular priority on ensuring that all personnel in the organization are both appropriately trained and on guard against cyber-attacks. Survey results suggest there is considerable scope for improvement in this area.

Area	Specific findings			
Risk Appetite (Q2)	52%	**Satisfied or very satisfied that Risk Appetite statement reflects Board's position on Cyber Resilience** *(PubCo: 100%; Cos>€1b:75%)*	17%	**Do not have a statement of Risk Appetite** *(FS: 4%; Charities: 26%; Cos<100k: 50%)*
Staff understanding (Q4)	58%	**Satisfied or very satisfied that personnel understand priority Board places on Cyber Resilience** *(PubCo: 82%; Cos>€1b: 63%)*	11%	**Have not communicated with their personnel** *(FS: 4%; Charities: 26%; Cos<100k: 33%)*

Board Member Responsibilities – Oversight

While the detailed business of managing cyber risks rests with management, Board Members' oversight must ensure that key elements of risk management are being implemented to their satisfaction. The survey probed four key areas to provide insights:

- confirming that **assets** that need to be protected are identified
- identifying the range of **risks** to which they are exposed
- selecting and implementing appropriate cyber security **controls**, and,
- building a capability for **Cyber Resilience** (the ability to bounce back from inevitable attacks)

In all four areas, survey results provide only limited assurance – overall levels of confidence about the adequacy of existing arrangements are modest. In particular, **the finding that as many as one in four Board Members are not aware of having had any incidents/near misses is particularly worrying.**

Area	Specific findings	
Affected assets (Q10)	29% **Boards endorsed listing of assets requiring protection within last year** *(PubCo: 73%; Cos>€1b: 50%)*	55% **Have never endorsed such a listing** *(PubCo: 38%; Cos>€1b: 48%; FS: 48%; Healthcare: 64%)*
Range of cyber risks (Q6)	20% **Extremely or very confident aware of the full range of cyber risks** *(PubCo: 36%; FS: 29%)*	26% **Not so confident or not at all confident** *(PubCo: 0%; Cos>€1b: 13%; FS: 19%; Healthcare: 23%)*
Cyber security controls (Q3/7)	26% **Extremely or very confident about adequacy of controls** *(PubCo: 55%; FS: 40%)*	56% **Somewhat confident about adequacy of controls** *(PubCo: 36%; FS: 56%)* 24% **Not aware of having had any incidents/near-misses**
Cyber Resilience capability (Q8)	54% **Satisfied or very satisfied about ability to deliver Cyber Resilience** *(PubCo: 82%; Cos>€1b: 76%; FS: 65%)*	10% **Dissatisfied or very dissatisfied about ability to deliver Cyber Resilience** *(PubCo: 9%; Cos>€1b:26%)*

Formal Assurance

The survey examined two potential sources of assurance for Board Members: management and external providers. Three in five respondents had received formal confirmation from management about the adequacy of cyber security defense in the last year; one in three have never received any such confirmation.

On external independent testing, the picture is also very mixed: about half of the respondents indicated that they had received results of independent testing within the last 12 months, half had not (including a surprising 27% of Public Companies). **When 'bad actors' require only a single click to compromise security, the importance of rigorous external testing is obvious.**

Area	Specific findings			
Confirmation from management (Q12)	58%	**Formal confirmation about adequacy of cyber security in last year** *(PubCo: 82%; Cos>€1b:88%)*	30%	**Have never received formal confirmation from management** *(PubCo: 18%; Cos>€1b:0%; FS: 15%; Charities: 63%)*
Independent external testing (Q9)	50%	**Received results of independent external testing in last year** *(PubCo: 73%; Cos>€1b: 51%)*	50%	**Received no reports of independent testing in last year** *(PubCo: 27%; FS: 46%; Charities: 84%)*

4. Case Studies

Case Study 1 – the "Silly Click"

"It doesn't matter how much training you deliver, how many reminders you send, how many glossy posters you put up, your staff will always be vulnerable to the 'Silly Click' – falling victim to a phishing attack.

There is no such thing as complete lockdown (sound familiar?). Some companies impose restrictions on what sites can be visited by their staff, or impose a blanket ban (for example, in some financial services companies), but that does not stop all forms of attack: for example, a 'man in the middle' attack or a masquerade attack can compromise your network just as quickly.

That's why we gave up a long time ago assuming we could ever keep all the bad guys out. Of course, we try hard to promote the right type of behaviour among our users (we follow-up on phishing tests by sending a second phishing test and then interviewing those that click a second time). Even then, the best companies struggle to reduce the 'Silly Click' to less than 15%. Less disciplined organisations can see over 40% of users clicking. We found it essential, therefore, to ensure we had appropriate resilience plans in place: it's not a matter of stopping every attack, it's making sure you can respond quickly to the one that gets through."

Irish CIO (Anonymous)

Case Study 2 – "This is not going away!"

"Three things worry me about cyber: people, technology and third parties.

People are probably the weakest link. No matter what rules you lay down (for example, not sending company information to a personal DropBox), you'll always find the exception that does.

Our technology defences have been strengthened considerably but, to use the old phrase, 'we're only as strong as our weakest link'. The only way to get decent assurance is to use the best industry standards and to get independent external testing. Even then it's a game of leapfrog to stay at least half a step ahead of the bad guys.

While many put a huge premium on using trusted cloud services (SaaS), the exposure from third party contractors is often underestimated. Their risk is my risk. If we don't exercise enough control over third parties, we become as susceptible as they are.

Boards think technology will save them but we're beyond that: the bad guys are keen to use technology to outfox even the smartest defences. We just have to improve our Cyber Resilience."

Executive Director (Anonymous)

5. Where to now?

Consider this thought experiment: imagine, one year from now, your Board Chair calls to tell you that the organisation has been the victim of a major cyberattack (take your pick from a ransomware attack, a denial of service attack, a major fraud or a malicious attack that paralyses your systems).

Your immediate reaction might be to consider:

- how to protect staff, customers, suppliers, others who may be directly or indirectly impacted
- the potential financial impact on the organisation (and whether you can recover any of the loss)
- whether, or the extent to which, you can continue operating without essential systems and data
- adverse press coverage and consequent fallout with key stakeholders and long-term reputational impact
- regulatory investigation and the possibility of regulatory fines

How well would you cope?

If subjected to detailed scrutiny, what gaps might be revealed in what you or your Board had done in the months leading up to the incident?

A thought experiment like this – examined now – is a good way of identifying the need for prompt remedial action.

To assist in identifying initiatives appropriate to your circumstances, we have set out below **10 key questions** for you to ask at your next board meeting and **10 suggested initiatives** for your consideration for the next 12 months. Of course, Board Members will need to prioritise which of these questions and initiatives are most relevant and appropriate to their Boards/organisations (recognising the extent of exposure, expectations of key stakeholders, available resources, etc.).

Further guidance

For additional Board Member guidance on strengthening Cyber Resilience – and further detailed materials – please go to: **www.ics.ie/cyberresilience**.

> "How do stakeholders know if an entity takes cyber resilience seriously? Currently they don't."
>
> *Cyber resilience is critical for organizations survival. World Economic Forum, July 2020*

> "In the future , familiarity with cyber security will become de rigeur for most directors."
>
> *Sam Curry, Harvard Business Review, November 2017*

10 key questions for Board Members to ask

1 Roles and responsibilities

As a Board, how can we be certain that we are aware of all our obligations when it comes to cyber security and resilience? And that all actions requested by the Board have been fully implemented by management?

2 Compliance with emerging Stakeholder obligations/ expectations

How do we ensure we comply with emerging stakeholder expectations (for example, where customers seek assurances from us about our Cyber Resilience)?

3 'Tone from the Top'

As a Board, how can we provide greater leadership in embedding Cyber Resilience in the organization?

4 Training

What training should we arrange for Board Members, individually and collectively?

5 Short term priorities/ emerging issues

How do we get regular assurance that the organisation is monitoring emerging cyber risks and taking immediate steps to deal with them as they become evident?

6 Adequacy of protection/ framework

How can we strengthen our Cyber Resilience processes?

7 Timely reporting to the Board

How can we strengthen reporting to the Board?

8 Directors' and Officers' (D&O) cover/cyber insurance

What type(s) of insurance do we need to cover the potential costs that may arise from the range of cyber threats we face (that we are unable to mitigate)?

9 Responsiveness

How can we improve the Board's ability to understand and respond to cyber-attack scenarios (for example, through table-top simulations)?

10 Funding

What additional funding is required to ensure Cyber Resilience aligns with our statement of risk appetite?

10 suggested Board initiatives

1 Agenda and resourcing

- **Make Cyber Resilience a standing item on the agenda**
- **Commit more resources**

2 Assurance

- **Get a deep-dive update on Cyber Resilience from management (to the Audit Committee or to the Board directly)**
- **Ask IT for a list of key risks and safeguards**
- **Increase audit frequency and scope (against relevant standards/guidance*)**

3 Basics – assets/risks/controls

- **Carry out a comprehensive refresh on the adequacy of controls (explicitly examining fraud, GDPR etc.)**
- **Enhance protection of intellectual property from theft**

4 Back-up

- **Strengthen (and test) back-up and continuity arrangements**

5 Independent testing

- **Enhance external testing (including 'Red Hat' testing, phishing, ransomware etc.) and rigorous 3rd party attestation**

6 Intelligence sharing

- **Join intelligence sharing platforms**

7 Investment in Cyber Resilience

- **Invest further in Cyber Resilience including enhanced reporting to the Board (especially on attacks suffered)**

8 Risk assessment

- **Conduct a thorough review of risks with deep board engagement – and decide on a proportionate response**

9 Training

- **Review training needs (especially for the Board) and deliver targeted training accordingly**

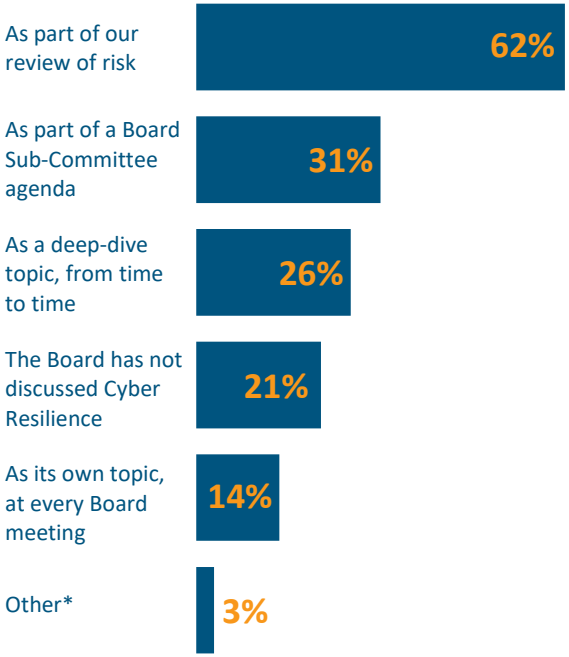
10 Working from home

- **Continue to address evolving cyber risks for home workers – especially use of personal devices**

* For example: ISO 27001, ISO 31000, NIST, Basel Committee, etc.

Appendix – Survey Response Data

1. As a Board, we examine Cyber Resilience:



* Construction, Public Administration, Energy, ICT, Manufacturing, Real Estate, Utilities

	Very satisfied	Satisfied	Neither satisfied nor dissatisfied	Dissatisfied	Very dissatisfied		
2. How satisfied are you that your Statement of Risk appetite reflects your Board's position on Cyber Resilience?	10%	42%	20%	10%	2%	17%	We do not have a formal Statement of Risk Appetite
3. How satisfied are you that the Board understands the reasons for cyber near-misses and incidents in the last 3 months?	9%	37%	18%	9%	2%	24%	I am not aware we have had any cyber near-misses or incidents
4. How satisfied are you that the Board has ensured that your organisation's personnel understand the priority the Board places on cultivating Cyber Resilience?	17%	41%	16%	13%	2%	11%	N/A – we have not communicated to personnel about Cyber Resilience
5. How satisfied are you with the training in cyber risk you have received, in the last 12 months, as a Board Member?	7%	27%	14%	18%	2%	31%	I have not received any training on cyber topics
8. How satisfied are you with the ability of your organisation to deliver appropriate Cyber Resilience?	6%	48%	28%	8%	2%	8%	Unsure – I don't have enough information

	Extremely confident	Very confident	Somewhat confident	Not so confident	Not at all confident		
6. How confident are you that you are aware of the full range of cyber risks that could impact your organisation?	1%	19%	46%	21%	5%	8%	Unsure – I don't have enough information
7. How confident are you about your organisation's cyber security controls?	2%	24%	56%	9%	2%	7%	Unsure – I don't have enough information

	More than 4	2 to 4	1	None
9. In the last 12 months, how many reports of testing of your cyber defences has your Board received from an external (independent) body?	2%	16%	32%	50%

	In the last 3 months	4 – 12 months ago	More than a year ago	Never
10. When did the Board last endorse an inventory of essential assets (provided to the Board by Management) requiring protection from cyber threats?	6%	23%	16%	55%
11. When was the Board last briefed on the organisation's exposure to cyber security threats resulting from third party contracts?	24%	27%	17%	32%
12. When did you last receive a formal confirmation from Management of the adequacy of your cyber security defence status?	29%	29%	12%	30%
13. When was the Board last briefed about intelligence-gathering on cyber-risk?	22%	19%	15%	44%
14. When did you (personally) last participate in a test of your (Board) cyber-incident plan?	7%	11%	9%	73%

ICS THE SOCIETY FOR CHARTERED IT PROFESSIONALS IN IRELAND

www.ics.ie
The Irish Computer Society, 87-89 Pembroke Road, Dublin 4, D04 R266
01 237 7723