Aldar Audit Bureau
Abdullah Al-Basri & Co.
Member firm of Grant Thornton International Ltd.
Grant Thornton

in association with Skillmine
Skillmine
Technology ▪ Consulting ▪ Services

Cyber-security through board leadership

Navigating the role of the board in mitigating cyber-crime

As organisations realign their operational models in the wake of the pandemic, several industries have introduced a prolonged remote working model, which could last beyond the first half of 2021.

These new working models have enabled a more globally connected infrastructure, which has driven the volume of data being generated across borders, industries, and organisations.

Unfortunately, this has meant that cyber risk has increased as criminals exploit every opportunity to commit cyber crimes against individuals and businesses alike.

During this current period, business leaders have a heightened level of awareness in respect of potential elements which could create further risk to operations, reputation or which may generate further costs to the business.

Whilst cyber-crime is a prevalent challenge for management teams, board members must pay further attention to cyber security, which was further validated in a recent poll where 86% of respondents from Saudi Arabia believe that cyber security should be a priority for board members.

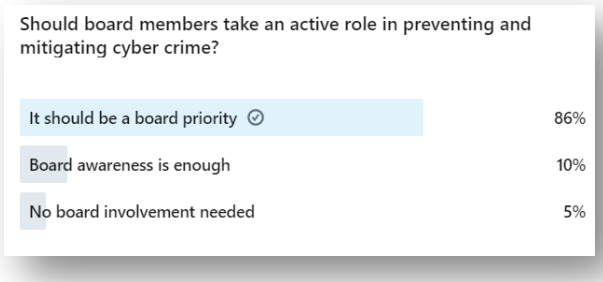


Figure 1. LinkedIn Live Poll Research

Cyber risk-management, across people, processes and technology, is now a fundamental for every business striving to grow and prosper in a connected, digital world. No business – whatever its size or sector – is immune. Boards have a key role to play in ensuring an effective strategy is in place. This report explains why and how.

1 Aldar Audit Bureau - Cyber-security through board leadership

Time for action

Now must be the time for boards to take action on cyber security. In this report we explore:

• where businesses are most likely to be vulnerable in the current climate

• identify the actions which board members need to take in order to manage and minimise risk and losses

• assess which board member is best placed to take responsibility of cyber-security.

Abdullah Al-Basri
CEO & Managing Partner
Aldar Audit Bureau - Grant Thornton, Saudi Arabia

The growing threat: who's affected?

The changing scale and nature of cyber-crime means every business is now a potential target, no board can afford to ignore the threat.

A new era of cyber crime

It is easy to imagine that cyber criminals are all highly skilled tech professionals. This idea could not be more wrong. Today, unnerving as it may sound, anyone can become a cyber criminal. Online videos providing detailed instructions on how to prepare an attack are only a click away for anyone looking to become part of the new cyber-crime wave.

With many of the technical and knowledge barriers to planning and executing a cyber-attack all but gone, cyber-crime is happening on an industrial scale. Meanwhile, vulnerability identification software has made criminal groups more dangerous than ever. The software enables groups to trawl IP addresses and identify unsecured systems with ease.

> The expansive exchange of data generated through remote working has become a valuable asset for businesses and cybercriminals alike. Protecting this valuable asset is essential for business leaders.

Imad Adileh
Partner
Grant Thornton, Saudi Arabia

How cyber criminals make money from your business

Ransomware

Attackers install software to shut down business systems or take the business offline. A ransom must be paid before the 'ransomware' is removed or deactivated. In a variation, attackers threaten to corrupt data and make it unusable if no ransom is paid.

Data theft

Attackers steal customer data and sell this on to other criminals to enable identity theft. Alternatively, they ask for a payment to release the data back to the business in a usable form.

CEO fraud

Online reconnaissance of publicly available data enables criminals to impersonate the CEO or finance director. Criminals can then request changes to payment details on invoices and divert payment to their own accounts.

Bitcoin mining

A relatively new but increasingly common form of cyber-crime. Attackers install software on the company's IT estate and hijack processing power to generate cryptocurrency. Business systems slow down or grind to a halt.

IP theft

Espionage isn't limited to state actors. Industrial espionage is a real threat, with ambitious companies targeting competitors' systems to uncover and steal IP.

> The cost of cyber-crime to businesses go beyond financial, impacting reputation, consumer confidence and employee sentiment. Mitigating such risks is imperative for business continuity.

Ahmed Al Zoubi
Advisory Director
Grant Thornton, Saudi Arabia

The impact of reputational loss on customer behaviour is real, with customers often switching to competitor brands following cyber breaches. In the B2B space, the fall-out from a breach may not be quite so public but is no less real. “When businesses cannot fulfil their contractual obligations because of a cyber breach, customers lose confidence and are likely to move to alternative suppliers.

Clean-up costs

The cost of cleaning up after a cyber-attack is a huge incentive to invest in an effective cyber security infrastructure. Dealing with the fall-out from a data breach, for example, demands a range of expertise on a scale that most mid-market companies do not have in-house. This includes digital forensics (to locate, assess, and repair the breach), law (to advise on regulatory exposure, contractual breach and liability) and PR management (to limit reputational damage). In the case of a data breach, a notification service to manage contact with customers whose records are affected, is essential.

Management time

The impact of a successful cyber-attack goes beyond the cost and reputational damage from business interruption. It also places a huge burden on the senior team, who will have designated roles in the incident response plan. During serious incidents, we typically see the CFO, the CIO and General Counsel committing 100% of their time until the crisis is resolved, and the CEO around 50%. Response activity may last for weeks, not days. The knock-on impact is considerable. Decisions are delayed and plans are put on hold as senior leaders’ attention is diverted away from their day jobs. We see the effect spreading across the organisation, with employees losing confidence in the leadership team and pride in the organisation.

Critical milestones of a cyber incident

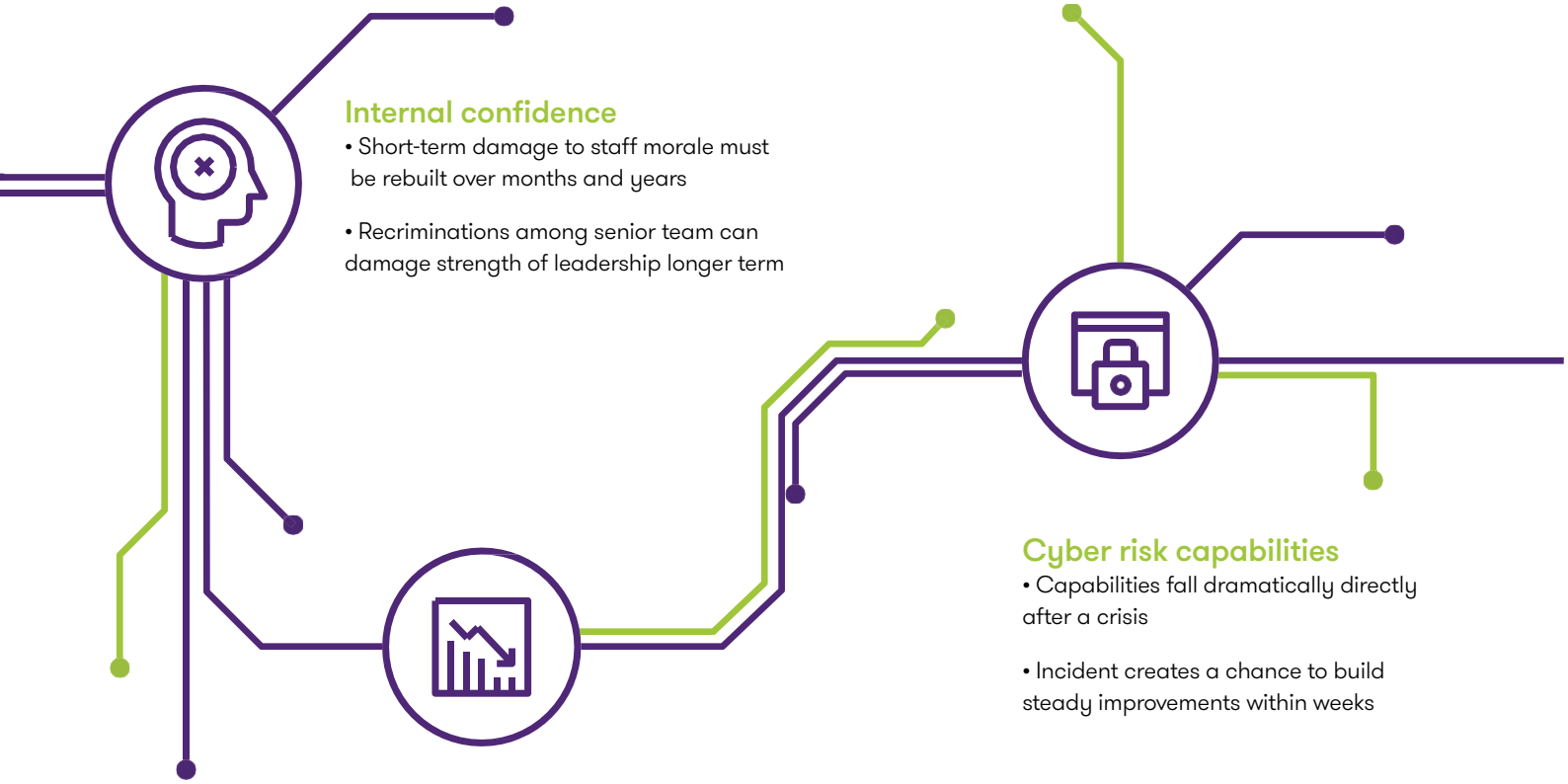
From our experience of working with clients post-incident, we recognise a number of recurring critical milestones that they, their staff, their brand and their clients experience.

Consumer confidence

- Immediate change in behaviours as consumers switch to alternative providers
- Takes years to rebuild to pre-crisis levels

Regulatory confidence

- An opportunity to improve regulatory confidence through effective crisis management
- Improvements can be achieved within days with the right actions



Internal confidence

• Short-term damage to staff morale must be rebuilt over months and years

• Recriminations among senior team can damage strength of leadership longer term

Cyber risk capabilities

• Capabilities fall dramatically directly after a crisis

• Incident creates a chance to build steady improvements within weeks

Business and operational capabilities

• Decision-making typically paralysed in the short term

• Recovery to pre-crisis capabilities may take many months

> If we could change our approach and thought process of the perceived cybersecurity threats and what is available to us, we can unlock our ability to truly excel in cybersecurity and mitigate these threats.

Fahad Alguthami
CEO
Skillmine, Saudi Arabia

Cyber Governance Maturity

As cyber threats continue to increase in prominence it has elevated to becoming a major business risk, which now requires input beyond the technical IT teams and current risk governance approach. Businesses must consider developing and adopting successful cyber risk management strategies, which will require board input. Businesses should consider their risk governance maturity and adapt procedures accordingly in order to ensure they are able to develop an integrated risk governance strategy in order to protect and react from a cyber threat effectively.

Characteristics of risk governance at different levels of maturity

Unaware	Managed	Embedded
• Business owners do not recognize or recognize the possible impact of cyber-attack; business decisions are made without regard to the risk. • In the IT department, security is implemented against its internally defined requirements and available budget and is not focused. • Cyber risk appears on the Risk Register, but the board is not regularly briefed on potential impact and threat, nor given adequate cyber training. • The board is not able to report accurately on cyber risk and management and has no cyber-attack crisis management plan.	• Cyber risk and effects are routinely defined by the company owners. • Cyber risk management is developed across organizations, IT and security and defines security business requirements. • Efficient surveillance is carried out to detect threats before completion of attacks. • Simple management information is given to the Board, allowing decisions on risk appetite and unsustainable events. • The board is periodically updated on threat and resilience; there is a high degree of expertise among key board members. • The Board is the controller of a cyber threat crisis management strategy.	• Cyber risk management and reporting is 'business as usual,' combined with a broader array of threats such as continuity of business and fraud. • Cyber risk management is increasingly quantified, allowing for a clearer evaluation and focused investment on protection. • The board is fully aware of internal and external threats, the management proactively manages risk in the context of threat intelligence and is flexible in response to threat changes. • All board members have the current skills to be involved in cyber discussions. • A crisis management plan is maintained and rehearsed. • All personnel acknowledge their role in supporting cyber risk management.

Board leadership makes the difference

Putting cyber risk onto the board agenda is one of the most effective ways to minimise the chances of a successful attack and reduce the financial impact if a breach occurs.

The neglected business risk

The growing threat, combined with the significant potential losses from a breach, makes cyber-crime an important business risk. But many boards are ignoring the danger.

More than six in ten of the companies surveyed say no board member has specific responsibility for cyber security. And in roughly the same proportion of companies, the board does not undertake a regular formal review of cyber security risks and management.

Why are so many boards ignoring this risk? In some cases, it is because board members are not fully aware of the severity of the threat from the current wave of industrial-scale cyber crime. This lack of understanding may go hand in hand with the lack of confidence many business leaders have in their ability to address the challenge. The temptation is to file cyber security as a technical issue and trust someone else is picking it up. This approach leaves the business exposed just as organised crime groups are ratcheting the risk up to a new level.

The temptation is to file cyber security as a technical issue and trust someone else is picking it up. This approach leaves the business exposed just as organised crime groups are ratcheting the risk up to a new level.

> Sophisticated criminals are constantly seeking ways to steal or corrupt private data, and it is the Board's responsibility to ensure that robust defences are in place to ensure protection of our business, our customers and our employees.

Mr. Brian Dickie
Director and Chair, Executive Committee
L'azurde

> Cyber risk needs to be considered just like any other business risk. What are the chances of it happening? What will the impact be? And how can we mitigate against it?.

James Arthur
Partner & Head of Cyber Consulting
Grant Thornton, UK

Reducing the impact of cyber crime

We know from experience that boards can make a real impact on reducing the likelihood of a successful cyber-attack and in minimising the reputational and financial impact when a successful attack occurs.

The three distinct areas where action by the board changes the outcome for the better, include:

- Review cyber security risks and management at board level
- Prepare an incident response plan
- Make cyber security the responsibility of a specific board member

Review cyber security risks and management at board level

Scheduling a regular and formal review at board level puts cyber security on the board agenda and ensures the issue receives the focus and investment it requires. Companies that do this suffer lower financial losses in the event of a successful attack.

Prepare an incident response plan

In responding to a cyber incident, a well-rehearsed plan of action can help business leaders act to manage a highly stressful situation quickly and more effectively, minimising business interruption and negative impact.

Our research shows that companies that have an incident response plan in place experience lower financial and reputational losses in the event of a successful attack than those that don't.

An incident response plan should cover the full lifecycle of a data breach–from discovery, to resumption of business as usual, to lessons learned. Our recommendation is that it should be rehearsed with a full simulated cyber-attack twice a year.

“

Cybersecurity threats are real and more pertinent these days. Organisations need to adapt counter measures to prevent Financial, Reputational & Regulatory damages. Prevention and management is successful when a top-down approach from Board Members is applied – this enables the right defence mechanisms to be created in order to manage the menace of cybersecurity threats.

Anant Agrawal
Managing Director,
Skillmine Technology Consulting

Make cyber security the responsibility of a specific board member

Making cyber security the responsibility of a specific board member helps to stop cyber risk management slipping through the net.

Companies most frequently choose the Enterprise Risk Management Team to fulfil the role. Yet, in our view, it's worth considering a different board member, without any particular technology specialism.

The Chief Financial Officer would be a good choice. In most mid-market companies, it is the CFO who is typically responsible for risk. Making cyber security their responsibility underlines the fact that cyber risk is a business risk, like any other, that needs to be managed.

There is a further advantage. In business, there is often a natural tension between operational targets and cyber security targets. Should the priority be to minimise interruption to operational systems (and therefore limit or delay software updates)? Or should maximum security be the priority, even if frequent updating means users cannot access business systems for hours or sometimes days?

A board member who is neither the COO or CIO has the benefit of a degree of distance on the debate and is perhaps positioned to find a better balance.

Who is involved in identifying, Prioritising, and assessing risk?

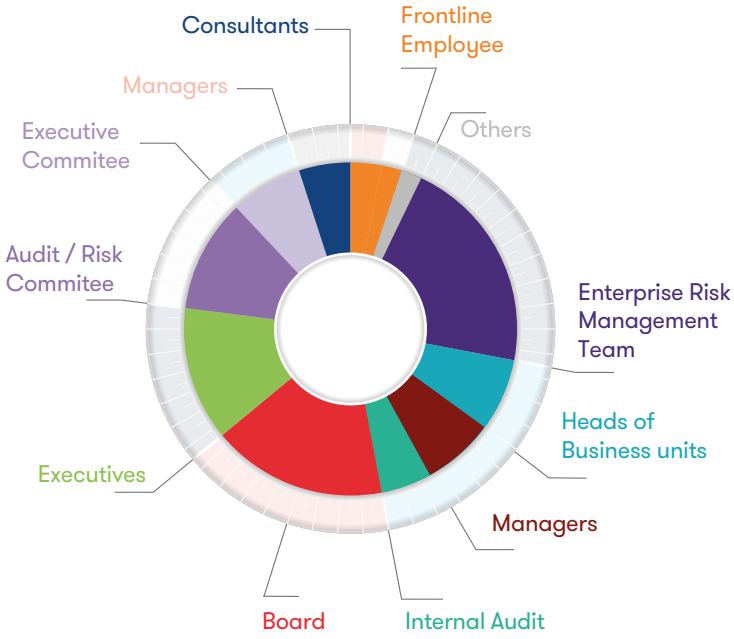


Figure 2. World Economic Forum Global Risk Reports, Kunreuther, Michel-Kerjan and Useem

Board Governance to mitigate the risk of cyber-crime

The stifling effect which a cyber-attack can have on a business is a strategic challenge which requires essential board leadership. Leaders are urged to consider:

Awareness

Board leaders require essential awareness of the threat which cyber-risks pose to them as senior executives, including their personal data and that of the business. This requires an audit of the value of data and cyber assets which are both vulnerable or a target of attack.

Responsibility

Whilst a majority of businesses assume the responsibility of cyber-protection remains within the remit of the technology function or CIO/CTO, the board must take wider responsibility for ensuring the business is protected, therefore it is important to either allocate responsibility of cyber-protection to a board member or enable the CTO a seat in the boardroom.

Strategy

A focused strategy is required which both simulates a potential attack and enables a swift response plan which will minimise the impact to the business and its associated stakeholders.

Supporting you to manage your cyber-exposure

Our team of local experts can support businesses to manage their cyber-exposure through our proven methodology, which includes:

Prepare

We help you understand your current exposure to cyber security risk and support you to develop an effective security capability. Our services include cyber security risk and threat assessments; security policy development; security -process or technical assessments; and third-party cyber security assurance.

Protect

We develop and implement the technical framework and broader processes required to protect. We can help you with security architecture; security technology implementations; security process design and implementation; identity and access management; privacy and data protection; data classification; enterprise application integrity; business continuity and disaster recovery; and penetration testing.

React

We work with you to support and monitor your cyber security operations and help you to respond rapidly and forensically in the event of a security or data breach.

Change

We can help you improve and better manage your cyber security capability. Our services include security programme strategy and planning, security governance; and security awareness.

Partnering for greater protection

The team at Grant Thornton Saudi Arabia have been working in alliance with Skillmine, a new-age technology solution provider. We support our clients to unlock greater value from the integrated cyber-solutions which are offered, that include:

Skillmine
Technology • Consulting • Services

Imad Adileh
Partner
Aldar Audit Bureau
Grant Thornton, Saudi Arabia
E iadileh@sa.gt.com

Ahmad Al Zoubi
Director
Aldar Audit Bureau
Grant Thornton, Saudi Arabia
E aalzoubi@sa.gt.com

About Us

Aldar Audit Bureau, Abdullah Al-Basri & Co. ('Grant Thornton Saudi Arabia'), is a member firm of Grant Thornton International Ltd. As one of the world's leading accounting and consulting firms we offer comprehensive assurance, tax and specialist advisory services to privately held businesses and public interest entities who span across a wide range of industries.

With over 30 years of experience in Saudi Arabia, we understand the needs of businesses who are dynamic, having worked with clients who range in size and industry. Our personalised local approach coupled with our global reach makes Grant Thornton Saudi Arabia the ideal advisers for organisations that are ambitious and who want to go beyond.

Visit grantthornton.sa today to find out how we can help you

I order to enable a seamless experience for our clients, whilst ensuring we provide a holistic solution that captures the entire cyber security, the Grant Thornton Saudi Arabia firm have engaged in a strategic alliance agreement with its partner of choice, Skillmine. This parnership enables our firm to provide and integrated approach for our clients and the wider marker.

Anant Agrawal
Managing Director
Skillmine Technology Consulting
E anant.agrawal@skill-mine.com

Ahmad Al Zoubi
CEO
Skillmine Saudi Arabia
E fahad.alguthami@skill-mine.com.sa

About Skillmine

Skillmine is a new generation IT Security, Consulting & Managed Services provider, helping customers to optimize their IT investments, while preparing them for the best-in-class secured operating model, for delivering that "competitive edge" in their marketplace.

We embark further on a journey to prepare our customers for the adoption of the best fit models and secured technologies, depending on their industry trends – be it Information security, IT Infrastructure, cloud adoption, Digital transformation, Robotic Process Automation, Application Development, Artificial Intelligence, Machine learning, GRC solution, SOC and NOC, and Data center consolidation etc.

Today, 450 + professionals are part of our family, with a wider presence in India, Saudi Arabia, UK, and the Americas. A growing list of marquee customers in various industry segments and consistent revenue growth epitomize our relevance in the market.

With thanks to our colleagues from Grant Thornton UK for sharing their insights and knowledge.

Aldar Audit Bureau
Abdullah Al-Basri & Co.
Member firm of Grant Thornton International Ltd.
Grant Thornton

grantthornton.sa