

A report from The Economist Intelligence Unit



Data security: How a proactive C-suite can reduce cyber-risk for the enterprise

The number one technology issue in the C-suite today is cyber-security.¹

And there's no wonder—attacks are becoming more numerous and more sophisticated than ever. The cost of cyber-crime to the global economy has topped more than \$445 billion²— equivalent to 1% of global GDP. Sometimes cyber-crime can seem unstoppable – while firms spent more than \$75 billion on cyber-defences in 2015³, cyber-crime grew by 38% that year.⁴

That's why C-suite executives everywhere are asking: What can we do to make a difference in defending against hackers, cyber-criminals and digital spies?

Research conducted by The Economist Intelligence Unit (EIU), sponsored by Oracle, provides answers. The results show that a proactive security strategy backed by a fully engaged C-suite and board of directors reduced the growth of cyber-attacks and breaches by 53% over comparable firms. These findings were compiled from responses by 300 firms, across multiple industries, against a range of attack modes and over a two-year period from February 2014 to January 2016.

The lessons are clear. As cyber-attackers elevate their game, the response must be an enterprise solution. Only C-suites and boards of directors marshal the authority and resources to support a truly enterprise-wide approach. In sum, proactive cyber-security strategies, supported by senior management, can cut vulnerability to cyber-attack in half.

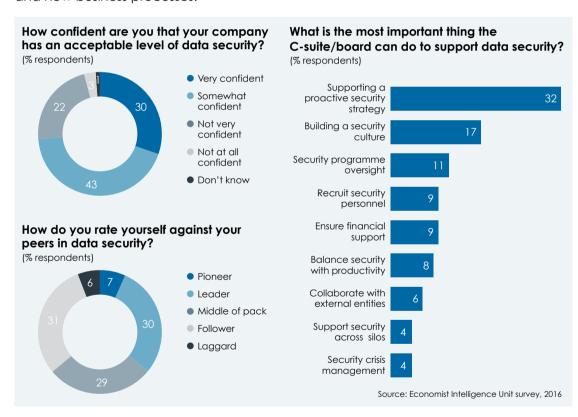
Sponsored by



The payoff for being proactive

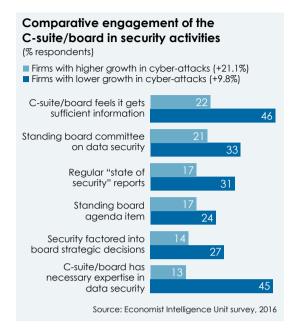
The EIU survey respondents were all members of the C-suites or boards of directors of their respective companies. They represented medium to large businesses in over 20 verticals, with equal representation from Europe and the Middle East, the Americas and the Asia-Pacific region. (See the appendix for more demographic details.)

The collective responses show the factors that differentiate enterprises with a high degree of success in cyber-security from those that continue to struggle. First, successful firms rely on proactive security strategies. Executives at companies with a high degree of confidence in their defences describe themselves as having a proactive data security strategy that goes beyond traditional approaches that rely primarily on reactive perimeter defences managed by IT departments. Instead, proactive strategies actively monitor external threats and mobilise the entire workforce to stave off attacks. In short, these approaches combine both the latest security technology and new business processes.



"Proactive security determines the impact of a breach, what data was actually disclosed, and the cost associated with it. It's more thoughtful and less emotional than traditional approaches," says Ron Woerner, director of cybersecurity studies at Bellevue University.

Second, successful security hinges on proactive C-suites and boards of directors. Why is the involvement of the C-suite and board so important?



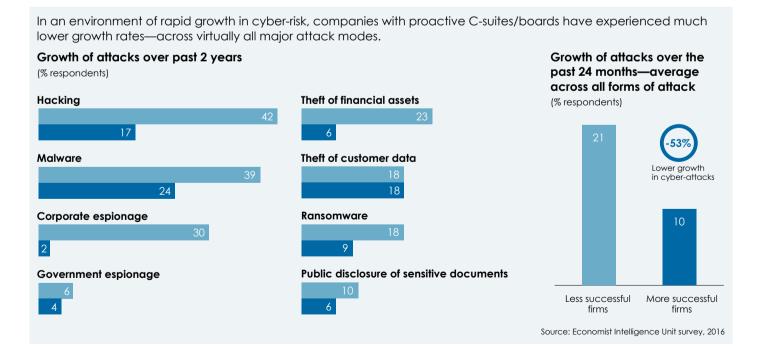
Part of the answer stems from the new kinds of threats organisations are facing today. Criminals attack all parts of the enterprise and frequently include penetrations launched through third-party suppliers and customers. These broader, more complex threat parameters require action from executives with oversight into the entire enterprise.

That demands a C-suite-level response. These leaders have the authority to mobilise all parts of the organisation, including appropriate responses from suppliers and partners. Just as importantly, senior executives provide budgetary and other resources to help ensure the success of proactive strategies.

"Boards become actively involved in security when they realise that security drives revenues and customer loyalty," says Jeffrey Ritter, external lecturer at the University of Oxford and author of the book Achieving Digital Trust. "If partners or customers are not confident about how secure your business is, they will decide to not do business with you."

For reasons like these, senior-level involvement is a clear indicator of cyber-security success, as the research data shows.

The payoff isn't confined to just responding more effectively to an attack—the influence of proactive C-suites also contributes to a significant reduction in the growth of cyber-attacks themselves.



Less successful: Firms with higher growth in cyber-attacks (+21.1%)
More successful: Firms with lower growth in cyber-attacks (+9.8%)

Overall, companies with proactive strategies and highly engaged senior executives are cutting the rate of growth of cyber-attacks in half, which significantly reduces exposure to cyber-attack risks, according to the EIU research.

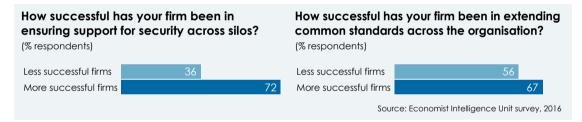
Six steps to a more effective cyber-security strategy

The benefits of proactive, C-suite-driven security are clear, but what are the essential elements to focus on when creating a plan? The following six steps correlate with high rates of deterrence of cyber-attacks and, tellingly, all are within the responsibilities of the C-suite and board of directors.

1. Align the organisation to support security

Key drivers of cyber-deterrence include reducing organisational barriers to security implementation and ensuring common standards across the enterprise. The process starts with breaking down silos. This addresses leading causes of security breakdowns, including fragmented security solutions. Silos also create gaps in coverage and force organisations to set protection at the level of the lowest participant.

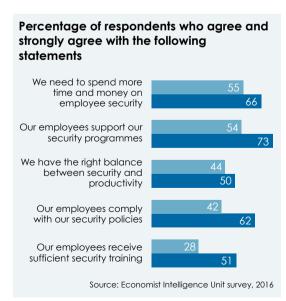
The next step in organisational alignment is implementing common standards across the organisation. This enables an integrated defence, makes security easier to manage and measure, and encourages organisations to adopt the highest shared standards for all departments.



2. Ensure employee buy-in and compliance with corporate security practices

Companies that have been more successful in deterring attacks have a stronger track record in these two important areas.

Employee compliance is essential for cyber-security success since this group continues to be the largest single cause of breaches, according to multiple industry studies. But tough compliance mandates alone aren't enough. Organisations must understand any road blocks that are keeping employees from strictly following

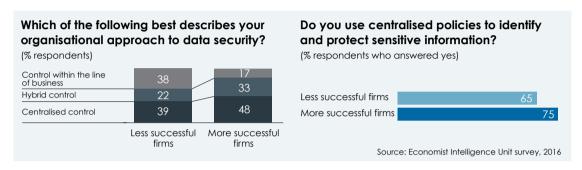


Less successful: Firms with higher growth in cyber-attacks (+21.1%)
More successful: Firms with lower growth in cyber-attacks (+9.8%)

policies. In particular, focus on whether employees are impatient with security procedures because they're seen as hampering productivity. Also, many organisations will benefit from additional employee training to ensure people understand the importance of security policies and have the knowledge to follow them completely.

3. Create a strong centralised management structure for security

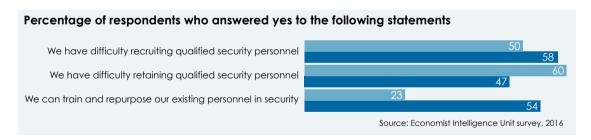
Companies that have been more successful in deterring cyber-attacks place a stronger reliance on centralised control over security programmes.



The reasons for centralised security are clear. Organisations can implement integrated systems that reduce the chance of security gaps that provide entry points for hackers. In addition, centralisation makes it easier to adopt common standards and enterprise-wide detection and monitoring of intrusions. Other benefits include simplified training and policy management, as well as cost efficiencies that come with not procuring and maintaining multiple security systems.

4. Meet skills shortages by retraining in-house personnel

Attracting and retaining skilled security talent is a challenge for any organisation. But successful firms are taking steps to address this long-time problem.

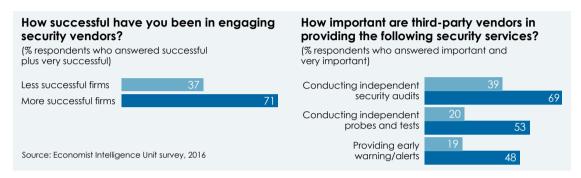


Notably, successful firms are meeting the challenge of recruiting data security experts by elevating the security skills of existing employees. These staff members have strong incentives to hone their security skills. Not only will it make them more effective for their current employers, but it's a smart career move. One study found that by 2019, a skills gap will leave 1.5 million cyber-security jobs unfilled⁵. "Over time, effective security has become less about just technology and more about integrating security into the processes of the firm," says Mr Woerner.

Less successful: Firms with higher growth in cyber-attacks (+21.1%)More successful: Firms with lower growth in cyber-attacks (+9.8%)

5. Tap the expertise of third-party security firms

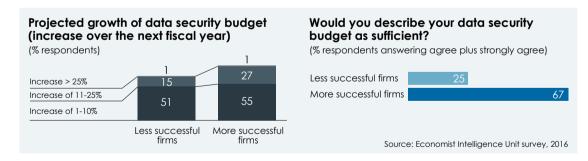
Given the size and complexity of the cyber-security challenge, internal resources alone may not be enough to fully defend against cyber-criminals. Successful firms supplement their internal security resources with third-party vendors. These providers offer an independent view for monitoring the effectiveness of a client's defences. Just as importantly, because third-parties engage with a range of customers, they bring a broad perspective on trending threats, as well as the latest best practices for keeping organisations protected.



"If I'm an independent threat-intelligence service with 5,000 clients, I have an opportunity to see new patterns of behavior before they become widely known by others," says Mr Ritter. "I know of one service that updates its black list every 30 seconds, and to do that, they're looking at over 275,000 nodes, including 50,000 honey pots, or decoy systems, that they manage to monitor the activities of hackers."

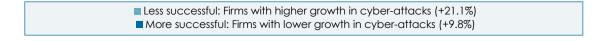
6. Invest sufficient resources—in particular, security funding—to meet today's complex data-security requirements

Despite cyber-attacks increasing by nearly 40% in 2015, budget increases remain modest. On average, enterprises are increasing spending by less than 10%.



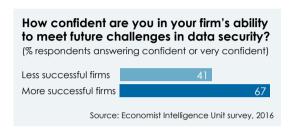
It's no wonder that IT staff at many firms feel outgunned and outspent by cybercriminals.

The EIU study found a significant correlation between low levels of funding and a lack of success which, as shown in earlier charts, also correlates with higher growth rates of attacks.



A ray of hope

As cyber-crime evolves, the role of the C-suite and board of directors is becoming vital for successful security efforts. Traditional static defences—characterised by "defending the firewall"—are becoming less effective as the volume and sophistication of attacks increase. The new era of cyber-crime prevention calls for a more elastic, proactive and cross-enterprise set of defences.



This in turn calls for mobilising employees, partners and external firms. Make no mistake—the answer isn't just another IT initiative. An effective, proactive strategy must mobilise almost the entire firm. Only the C-suite/board has the authority to support this level of engagement for the long term. But as the EIU data shows, this

modern approach pays off in a significant decrease in the number of cyber-attacks on the enterprise.

There's one other benefit—greater peace of mind.

Firms that are pursuing proactive security strategies with strong C-suite backing are more confident about the future—it's a welcome contrast to the litany of discouraging news that often surrounds cyber-security.

[■] More successful: Firms with lower growth in cyber-attacks (+9.8%)

Appendix: summary of survey demographics

In February-March 2016, the EIU surveyed 300 executives identified as responsible for or are knowledgeable of cyber-security in their companies. The following is a summary of survey sample demographics.

Seniority and function

Company leadership, strong IT representation (% respondents)



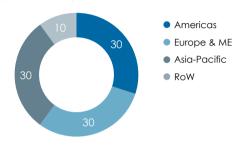
Size of company

Medium-large business—supports complex IT (% respondents, US\$bn)



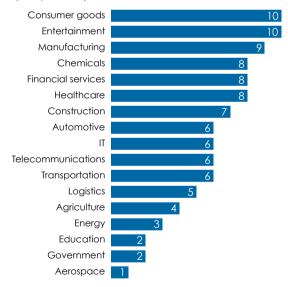
Geography

Globally representative by region (% respondents)



Industry

20 verticals, none more than 10% effectively represents all industries (% respondents)



- 1 http://www.industryweek.com/strategic-planning-execution/10-questions-leading-boardroom-agendas-2016
- 2 http:co//www.telegraph..uk/technology/internet-security/10886640/Cyber-crime-costs-global-economy-445-bn-annually.html
- 3 http://www.gartner.com/newsroom/id/3135617
- 4 http://www.pwc.com/gx/en/issues/cyber-security/information-security-survey.html
- 5 http://searchcio.techtarget.com/news/4500273059/Obamas-19B-cybersecurity-plan-takes-aim-at-cybercrime-underscores-skills-gap