TIME TO INVEST

Spencer Young *examines the importance of convincing the board to invest in cyber security before it's too late*

Even if you weren't glued to HBO's chilling *Chernobyl* mini series, you'll probably know the rough outline of the worst nuclear disaster in history. A poorly planned 'safety' test revealed, in the most catastrophic way imaginable, the fundamental inadequacies of the Soviet RBMK nuclear reactor. The resultant massive explosion took the roof off and exposed the burning reactor core to the atmosphere – with consequences that are still being felt to this day and will carry on being felt well into the future.

When it comes down to it, compared with Chernobyl, a security breach is pretty small potatoes. Yet it can still cost people their jobs, cause irreparable reputational damage to the organisation, and can even be enough to send people involved to jail, as witnessed in recent years.

Board members are responsible for establishing good governance practices and policies

The disaster in 1986 has much in common with a data breach. It's not just the metaphor of the heart of the installation being exposed to the environment; it's that, like many breaches, the seeds of the Chernobyl catastrophe were sown long before disaster struck. The workers at the plant didn't know it, but they were sitting on a powder keg, unaware that a single spark could set the whole thing sky-high.

Disasters are usually followed by enquiries and, where necessary, new laws and regulations to prevent them from happening again. Chernobyl sparked much soul searching in the Soviet Union, contributing to *glasnost* and, ultimately, the fall of communism. Similarly, our ever-growing data gathering and a spate of high-profile breaches led to the creation of new regulations such as GDPR, designed to prevent large-scale data disasters or at least to mitigate their effects.

FALSE SENSE OF SECURITY

Businesses around the world may have spent billions on making preparations for GDPR, but achieving compliance is not a guarantee that future breaches will be prevented. In fact, there is a worry among cyber security experts that GDPR is actually lulling businesses into a false sense of security.

Indeed, one year on from the implementation of GDPR, the UK's Home Office has just revealed a massive spike in the department's reporting and recording of data breaches. The Information Commissioner's Office recorded 35 individual breaches in the year to 31 March 2019, up from two in the previous year. While this spike is doubtless down to the more robust reporting requirements mandated under GDPR, it shows that the regulations themselves are not necessarily enough to eradicate data security disasters. More has to be done to ensure organisations are fully equipped with the right processes to ensure that breaches do not succeed.

In particular, this highlights the challenge facing CISOs: how to convince the board to maintain or increase their investment in cyber security at a time of heightened threat. As well as how to explain that GDPR is, in many ways, a sticking plaster rather than a guarantee against future breaches.

These are exciting, turbulent times for business. Organisations in every sector are undertaking digital transformation projects that aren't just designed to deliver more efficient ways of working, but promise to transform the very nature of businesses, enabling them to branch out into new markets with an even greater array of products and services.

Compared with the consequences of digital transformation, security can seem a decidedly unexciting undertaking. Spending on security promises no guarantee of a return on investment; rather it's seen as insurance. With so many lines of business department clamouring for new technologies, it's easy to see why extra spending for security doesn't get a look in. But this doesn't mean that it is not an essential component for businesses.

Yet the CISO knows what the board doesn't: that smart spending on cyber security is never wasted, and that secure operations provide the very bedrock for the business' entire operations. Their job is to convince the board to spend the money required for this important but admittedly 'unsexy' area of IT.

This should be an easy win, in theory. Board members are ultimately responsible for establishing good governance practices and policies for driving better financial performance and growth. Any security breach threatens to undo years of hard work in an instant; meanwhile, it's possible that those who ignored the CISO's warnings could be held accountable and face fines or even jail terms if they deliberately choose not to make the required cyber security investment.

Where cyber security may have previously been considered one subset of operational IT, the growing number of breaches in recent years should ensure that security becomes imperative to even the most purblind board members.

CISOS MUST ENSURE THAT SENIOR LEADERS ARE AWARE OF THE GROWING THREAT THEY FACE EVERY DAY

Last year, for example, a report released by the Department for Digital, Culture, Media and Sport revealed that over four in 10 businesses (43 percent) in the UK experienced a cyber security breach or attack last year. The same report went on to highlight that despite the growing number of cyber security threats and attacks, fewer than three in ten businesses (27 percent) have formal cyber security policies in place. These are some examples out of many which showcase the need for more robust security practices to be implemented across all organisations.

While preparations for GDPR may have eliminated some of the organisation's security vulnerabilities and tightened up detection and reporting capabilities, anyone who believes that this is enough to guard against today's increasingly sophisticated cyber threats is living in a fool's paradise.

Of course, many organisations are well aware that the cyber security threat continues to grow, and that a data breach is all but inevitable. The danger is that the board believes that no amount of investment can possibly prevent a successful cyber attack. So, what exactly needs to be done to change this perception?

This is where the CISO must focus their attention, moving the conversation beyond the traditional fear, uncertainty and doubt that traditionally characterises the conversation on cyber security. Instead, they must concentrate on the very real benefits that spending on the latest generation of security technologies can bring and identify how this investment can limit the scope of damage from a data breach.

One of the best ways of convincing the board is to remind them that liability for failing to govern risk and protect critical data is moving from the IT department to senior leadership. That alone should be enough to make the board sit up and take notice. But the goal is not merely to alarm; it is to educate and also to reassure. CISOs can mollify this initial

shock by discussing the specific risks and stressing the importance of quantifying, and therefore managing them effectively. Education is the source to ensuring that risks are mitigated.

Business leaders need to be able to measure risks in several areas, including compromised customer data, diminished brand and reputation and loss of investor and consumer confidence and loyalty. At the same time, they face the fallout of stolen sensitive intellectual property, potential compliance and regulatory sanctions and, beneath it all, everyday business disruptions that cost a fortune.

Once these risks are quantified, due diligence requires leaders to assess the steps that they and their partners are taking to avoid exposure. It's equally important to look at the competition and see where they are taking steps to prevent or mitigate potential breaches in the future.

Having built a comprehensive picture of the business' vulnerabilities and its potential exposure to a breach, it's time for the CISO to take the lead in addressing them. The good news is that they no longer have to do this alone. Most technology providers pride themselves on taking a consultancy approach and will therefore give their customers invaluable advice on the current threats within your marketplace, and can also help with the next stage of the process: the full security audit.

This audit should pinpoint exactly where the organisation's critical data currently resides, and who actually requires access to it. It might seem obvious, but many leaders don't understand the risks of a potential data breach by careless, compromised and malicious insiders. Not all data assets carry the same level of risk and not every employee should be given *carte blanche* access to all organisational data.

By appraising your data assets in terms of their value and risk, you can then begin targeting your investments towards timely threat detection and incident response. But in the constant battle to keep the board invested in the process, it's important this is framed in terms of risk and reward equation, with the assumption that a data breach is inevitable. By using a tiered security approach, your organisation can protect high-value targets that would cause significant harm if they were compromised.

CISOs must ensure that senior leaders are made aware of the growing threat they face every day from external cyber attacks and internal data breaches. A single breach has the potential to irreparably damage the financial condition of even the most successful business and ruin the careers of those leaders involved. Rather than packaging your cyber security spending rationale within IT investments, these really need to be highlighted as a high-level risk mitigation strategy.

All this hard work will make it much easier to target your investments towards timely threat detection and incident response. If CISOs can show how spending on specific technologies can counter specific threats, they will be much more likely to secure the investment they need to keep the organisation safe.

The approach of focusing on the dangers and senior board members' personal liabilities might seem like the 'nuclear option', but it's critical if the organisation is to avoid the potential meltdown that could come from a successful cyber attack ●

Spencer Young – Regional Vice President EMEA at Imperva – is dedicated to helping IT security professionals realise tangible business value from their security technology by delivering meaningful and actionable insights to Data and Application activity.

The question is not can you afford to invest in cyber security, but can you afford not to...