Who's to blame for a data breach?

By Sooraj Shah
12 Nov 2015

It is no longer a shock when a huge company is hit by a crippling cyber-attack, which exposes details of millions of its customers - at least not from an industry perspective.
The end result, though, isn't only damage in terms of customer trust, but millions of pounds spent on lawsuits, settlements and compensation. But for some of the organisation's employees, it doesn't stop there: the CEO, the CFO and the CIO will all have their hearts in their mouths if their organisation suffers a data breach.

More than half of UK organisations are planning to increase their cyber-security spending over the next 12 months, according to consultants EY (better known as Ernst & Young). Some of this spending will be going on chief information security officers (CISOs), to give a named individual responsibility for heading up the security effort. Major companies, such as drinks company PepsiCo and global bank JPMorgan Chase, have been looking to recruit CISOs, as they strive to place a greater impetus on security.

For the bank's part, it was much too little, much too late. JPMorgan Chase was the subject of a catastrophic cyber-attack in July 2014, which compromised the data associated with more than 83 million accounts, including seven million small businesses. US officials this week told Bloomberg that the hack "was the largest theft of consumer data from a US financial institution in history" and four men have been charged over it.

Last week, Bloomberg reported that JPMorgan's chief security officer, Jim Cummings, had been re-assigned to a new position within the bank, following the company's major data breach. But Cummings may count himself lucky, as other directors have had to bear the brunt of the attack themselves - take the CEOs of Target and Ashley Madison's parent company Avid Life Media, for example, both of whom resigned following data breaches in their organisations.

The blame game
According to Patrick Seeber, CIO at chemicals and sustainable technologies company Johnson Matthey, everyone in the organisation should be collectively to blame for a data breach, not just CEOs.

"The approach we take in the organisation is that security is just like health and safety. It's every employee's responsibility to look after security. A big chunk of our time and approach is about awareness and training and being able to understand the risks that are associated with certain behaviours and getting people to behave in the correct fashion," he says.

"Certainly, IT is actively involved in addressing and fixing the problem and trying to sort it out. But in terms of prevention and identifying those risks, it's the responsibility of every employee," he adds.
In the recent case of a breach in Ireland involving the data of 300 civil servants, it was clear to see that one officer's "momentary lapse in concentration" was to blame.

But in the cases of both Target and Ashley Madison, senior executives have seemingly taken accountability for the hacks despite not directly being involved in the same way. Target's CIO, Beth Jacobs, was accused of knowing about the flaws in her department, but doing too little to minimise security risks, while Target CEO Gregg Steinhafel was criticised for taking computer security too lightly.

Perhaps because of the size of the organisations and the complexity of the hacks, it isn't as easy to pinpoint someone specific to blame - or, more likely, it isn't just one person's fault.

But even if certain employees lower down the chain of command were in some way at fault, many feel that senior members of staff should carry the can. At least, that's what Raytheon and Websense found in its surveys of attendees at an eCrime Congress in London in March.

The survey revealed that 70 per cent of attendees believed that CEOs should take the blame, with only 13 per cent believing it should be a CISO. But in a later survey in October, 60 per cent believed that the CEO should be blamed, with 33 per cent believing that the buck should stop with the CISO.

Fingers were also pointed towards IT departments and the employees directly responsible for any data breach.
So far, the CEO of TalkTalk Dido Harding has refused to bow to pressure to step down after the internet service provider's infamous data breach. Harding told *The Telegraph* that she has the full support of the TalkTalk board, including the chairman of the company.

But while she has support now, a full investigation into the breach may make the board and chairman think differently.

The CIO of estate agency PurpleBricks, David Kavanagh, believes that with any data breach there should first be a thorough investigation, in part to determine who, if anyone, ought to be blamed. If that means that person has to lose their job, so be it. But he said that it would be hard to identify and isolate one person as the sole cause of a data breach, as several factors are likely to lie at the root of the problem.

Seeber at Johnson Matthey believes sometimes staff are axed merely to appease shareholders. "The head of Volkswagen left [after the emissions software scandal] but I doubt he was aware of what was going on, and that comes with the territory, unfortunately," he says.

Seeber believes that either the CISO or CFO are likely to be accountable, at least in his organisation.
"It's going to be either the CISO or CFO, because the CISO reports into the CFO in our organisation. If we were to have a major breach in our organisation, the CFO would be the one standing up in front of the shareholders, telling them where we are, why there was a problem and what we are doing about it," he says.
"He will feel the pain, and that will very quickly shift on to me," he adds.

Seeber believes that the CFO and CISO are key in terms of embedding the right behaviour within the organisation.
"It's the same as health and safety. Is your health and safety officer responsible if there is an accident? Yes, they might pay the price in terms of not having the right procedures in place, but ultimately it's an employee's own duty [to look after themselves]," he suggests.

Coalfire's managing director, Andrew Barratt, agrees that employees should collectively take responsibility. C-level executives, including CIOs and CISOs, may preach that security is everybody's responsibility. They may also argue that if their IT security budget is slashed they might not be able to protect or monitor against the threats that are affecting them.

"If you're an executive and are not getting the information on risks you need to make timely decisions - does that put you at fault? Is ignorance bliss? How do we attribute blame?" asks Barratt.

But Barratt suggests that a "blame culture" is the last thing the industry needs. "Blame culture can lead to bad decision making as individuals are typically incentivised to dodge blame instead of managing risk," he says.
He continues: "If everyone feels like they are empowered to identify risk, and escalate this to executives who are armed with the appropriate information to make decisions, then they can truly be held accountable in the event of a large-scale incident."

This is why Target's CEO and CIO are no longer at the company.

The meaning of 'accountable'

But there are some C-level executives who are happy to take accountability. "We haven't got to that point [of a data breach] thankfully," says Reckitt Benckiser CIO Darrell Stein.

"But ultimately it's my accountability; someone has to be accountable for it. My job is to increase the awareness, make sure we are spending the right amount of money and getting those investments right as well," he adds.
But there is a difference between who's accountable and who loses their job.

CISOs or data protection officers may have clauses in their contracts that specifically state that they will be held accountable if the firm was to suffer a data breach, and that could put them at risk of losing their job even if they weren't to blame.

"The CISO, and likely the COO, [will] lose their job in the event of a large data breach, but they are not fully to blame," says Alexei Miller, managing director of global technology consulting firm DataArt.

"Guarding against cyber-theft in a large organisation is similar to guarding airports, only more complicated. We all take our shoes off and go through metal detectors. Now, imagine doing it 20 times a day. That would be infuriating, so short cuts would become necessary. Cyber-security is all about compromises with usability and customer service. The CISO is hardly to blame for those compromises," he suggests.

Consumers don't necessarily feel the same. Security company Bit9 + Carbon Black found that seven per cent of people that it surveyed actually wanted individuals in the organisation to be culpable for their supposed security failures. Indeed, their survey suggested that some people even wanted security officers to face jail time - indicating, perhaps, how much importance people place on their personal data (except, maybe, when they're handing it all over to Facebook and Google).

The challenge for many organisations is that they are being targeted by cyber-criminals frequently - they have no hiding place. In the aftermath of a data breach there are more important things to worry about than who exactly is to blame, and who should be held accountable.

There will be a damage limitation exercise from a PR standpoint, of course, as well as legal cases to worry about. It's also an opportunity to drive home the importance of security among staff across the organisation.
But when the dust settles, shareholders and consumers alike will no doubt want someone to take the blame. At least then, the organisation's tarnished reputation can start to be repaired in their minds.

That is why a thorough, transparent and honest investigation needs to take place by an independent third-party to determine what exactly went wrong, and who, if anyone, ought to shoulder the blame.

Original article — http://www.computing.co.uk/ctg/feature/2434299/whos-to-blame-for-a-data-breach