Why Security Fails: The Case for Risk Management

By Justin Somaini, Symantec CISO

If you don’t speak to the business in their language, then don’t be surprised when security is subverted in the name of “getting things done.”

As information security leaders, we tend to think a lot about the technical and the tactical: how to most effectively implement and manage firewalls, anti-virus software, network access controls and secure coding initiatives. On its face, there’s nothing wrong with that. After all, it’s our job to protect sensitive corporate and customer data. The problem comes when we believe business executives care as much about those things as we do.

CISOs who make that assumption set up their information security organizations to fail. If you’re focusing on technology details in your relations with business units and using fear tactics to try to force compliance, you’re missing a big opportunity to convince the C-suite of security’s importance to what they do care about: managing risks to revenue streams, operations and the brand.

Business leaders must be convinced of their responsibility for security as it relates to their efforts to promote the company’s success—which obviously includes protecting it from severe financial hits. And the impact of breaches on the bottom line can be considerable: according to a 2008 Ponemon Institute benchmark study, the average organizational cost of a data breach is $6.65 million.

To promote security as a valued business driver and enabler, CISOs need to develop governance structures and regularly share information with business leaders. That information should drive their awareness of security’s relevance at a strategic level and help them take action on issues that could put data—and the business—at risk.

Awareness and action

In many organizations, information security leaders interact mostly with directors or managers whose main goal is to get a project done fast. That has to change. Your discussions need to be with those who are highly motivated to protect the brand, the operations and the revenue stream: the CEO and business unit leaders to whom those directors and managers report. Those folks won’t feel so confident about taking shortcuts if they know their bosses are in your corner.

Try to schedule a half-hour with your CEO to present your case on the strategic function of information security. Explain why you should facilitate ongoing awareness about company-wide risks and proposed solutions. Do the same for top executives around business unit risks and proposed solutions. Here at Symantec, that awareness takes the form of regularly emailed reports about critical security concerns. Rather than stating a technical vulnerability and detailing how we’ll address it, the reports outline the potential business impact of the issue (financial, brand, operational) and provide a high-level explanation of how the InfoSec function has things covered. We also give them, as the responsible business owners, an opportunity to voice any concerns they may have with our plans.

This approach is important for the sake of your own brand as a CISO. You don’t want your business peers to view you as someone who’s always raising a fuss and demanding their time. You want to present yourself as having solutions for potential issues, while leaving the door open to further discussions about addressing business risks.

Certain issues will require more active participation from the C-suite, such as when a department wants a policy exemption for a project that your team thinks is a significant risk to the company. Your governance framework should include live meetings with the CEO or business unit owners—or empowered and accountable representatives—where you can debate the issue and decide on actions. As CISO you must make it clear that only business leaders can accept such potential risks on behalf of the company; indeed, you should step back and let the business representative(s) agree to that accountability by running the meeting.

Getting the C-suite to participate in security strategy is a big step towards reducing failures in the InfoSec function. Instead of being reactionary, InfoSec acts proactively. Instead of talking to the business in a language it can’t understand, InfoSec speaks clearly about business risks and how they can help manage them. Instead of being seen as a roadblock, InfoSec is at last seen as facilitating action and positive outcomes.
About Justin

Justin Somaini is Chief Information Security Officer at Symantec, responsible for managing all aspects of Symantec's information security strategy. Somaini plays a strategic role in protecting Symantec's IT resources and information assets and drives all internal security initiatives. Reporting to Symantec's CIO, Somaini has responsibility for Symantec's IT information security risk management, threat response, governance, and privacy functions.

Somaini has more than 12 years of information security and corporate audit experience with large organizations.