19 MAR 2013 MAGAZINE FEATURE

A CEO's Guide to Information Security Compliance

Constantly changing regulations require “board visibility to win the investment required to address them", according to Guy Bunker of Clearswift

Compliance is an ongoing challenge for businesses. According to one study, international organizations have to obey some 600 different regulations and laws in the information security space alone.

This administrative burden goes hand in hand with increasingly stiff penalties for non-compliance, such as in the UK, where the Information Commissioner’s Office can now impose fines of up to £500,000 (~$800,000) for data breaches.

Organizations face a compliance burden that is anything but fixed. Information privacy and security regulations constantly evolve, with regulators and lawmakers themselves admitting that they struggle to keep up to speed with technology developments such as cloud computing, or Big Data.

The increase in regulation is also coming from outside traditional information security quarters, as well as the modification and updating of existing laws. Large-scale data privacy reforms, such as proposed revisions to the EU's data protection regulations, will of course affect any organization doing business on that continent, but it may well reduce bureaucracy by replacing 27 national laws with a single framework.

New laws, such as the UK's proposed Data Communications Bill – which would impact businesses from telecommunications providers to social networks – are extending the scope of compliance. So will changes in guidance put forward, for example, by the US Securities and Exchange Commission (SEC). Listed companies in the US now need to take the protection of their intellectual property into account, as

urity vendor Clearswift points out, new – or significantly
come to the CEO's attention, if only because of the cost

et board visibility to win the investment required to address
's new guidance are also pushing security further into the
previous compliance regimes.

This is further adding to the compliance burden, as organizations might feel obliged, or pressured, to go beyond the law or their industry's regulations, in order to appear as ‘good citizens’. Examples of this trend include the recent decision by Starbucks to change the tax structure of its UK operations, in the face of public criticism, even though its existing arrangements were legal.

Within the information security field, it is already common practice for public sector and healthcare organizations in Europe to notify data losses to their local regulator – sometimes publically, sometimes in private – even though the law does not oblige them to.

Creating a Compliance Framework

For corporations, notifying the public or other stakeholders of a data loss event or a cybersecurity attack is increasingly seen as good practice, not least because swift action can limit any reputational damage.

"Ethically, it is certainly preferable to foster a culture that sees the security and privacy of customers as a benefit", says Lee Newcombe, managing security architect at Capgemini, a technology consultancy. "But there must be some underlying business benefit – even if only an improvement in reputation – to justify any investment."

The changes in the way organizations with the best reputations in security and data privacy view the issues reflect some of the underlying tensions between good security, risk management, and compliance. Laws around data protection, privacy and information security will always be developing.

"Risks change day by day whether it’s a new device or a new application, or how the business goes to market", notes Michael de Crespigny, CEO of the Information Security Forum (ISF). "Our members are finding it hard to understand what they are complying with, and sometimes, what the body of authority is."

A Pragmatic Approach

In practice, even well-run organizations might struggle to achieve complete compliance with all laws and regulations, in every territory, at any one time.

monstrating that they have taken steps to ensure compliance, elow) or other relevant standards, even though these uality.

rk is also prompting boards to take either a risk-based approach to compliance.

ght be in terms of complying with, or not complying with, ual, so you direct efforts to the areas of greatest risk", the ISF's

t efforts to the areas of greatest risk"

experts advise, needs to be aware of security and compliance issues, and promote that awareness across all levels of the operation.

If this has a cost, it should be offset by the protection it gives to the organization's reputation, as well as the readiness it brings when it comes to complying with new legislation.

Organizations with the right frameworks in place are less likely to be wrong-footed by new laws or compliance regimes. "If you apply good security practice, compliance should be part of that. Compliance standards often come out of good practice", explains Garry Sidaway, global director of security strategy at Integralis, a consultancy.

At the same time, however, CEOs need to remember that the compliance regime is rarely, if ever, static even when there is no new legislation in the pipeline. Compliance priorities will change as the organization's operations change, and as operational measures to support compliance reach a level of maturity.

As Clearswift's Bunker points out, as a new regulation, the Payment Card Industry Data Security Standard (PCI DSS) quickly became a board-level issue in the retail, payments and banking industries. Yet as the regulations matured and businesses adapted their processes to meet them, compliance largely moved down to business operations.

CEOs and their advisors – especially CISOs and heads of compliance – need to be flexible enough to stay ahead of new legislation, but also able to delegate compliance with the old.

"From a CEO point of view, you need to have knowledge and awareness of applicable legislation: there are CEOs with operations in lots of nation-states. They need to understand what the general [compliance] impact is", says Ken Allan, global information security leader at Ernst & Young.

But the CEO's role goes further, he asserts. "You have got to understand what's required beyond compliance with legislation, and to keep the organization secure." Implementing standards such as ISO 27001 (see box-out below) is a good start, he says, but it will not, on its own, ensure compliance.

> **"From a CEO point of view, you need to have knowledge and awareness of applicable legislation"**

eans looking at the inevitable tradeoffs that come with
than the cost of compliance, or less than the cost of the fix",
approach rather than a security approach prompts firms to
he cost", he warns.

IT [security] spend was adequate to get me to the right
r fines and, in some cases, potentially custodial sentences,
th about their organization's compliance, rather than keeping

Perhaps the key role for the CEO in compliance is ensuring those structures are in place. The IT security profession also needs to play its part in helping the CEO, by stating the issues facing the business, in business terms.

"IT security doesn't report in business language, but in terms of the number of vulnerabilities in systems", says Integralis' Sidaway. "What the board member wants to see is the impact on the business. If I fix this, what does it cost in terms of downtime or risk? That is board-level language."

If information security can put their case to the CEO in that way, organizations are likely to see not just their compliance, but their overall security performance, improve as a result.

What is ISO 27001?

ISO/IEC 27001:2005 is published and maintained by the International Organization for Standardization (based in Geneva) and covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations).

ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or their business units. Intended for different types of use, the standard is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties.

Source: International Organization for Standardization

Recommended for you

WhatsApp: Newest Attack Target for...

www.infosecurity-mag...

Teen hacker earns $60K for full Goo...

www.infosecurity-mag...

Related to This Story

Comment: Is Your Office Printer Secure?

Comment: Organizations Must Keep Up with New Compliance Regulations

US standards drive Canadian information security

A CEO's Guide to Risk Management

Security's Steering Force

What's Hot on Infosecurity Magazine?

Read Shared Watched Editor's Choice

1 24 OCT 2019 NEWS
AWS Left Reeling After Eight-Hour DDoS

24 OCT 2019 NEWS
y Industry is Stagnating

ion After Capital One Breach

ven Fuel App Breach

STRATEGY I INSIGHT I TECHNOLOGY

infosecurity
CONNECTING THE INDUSTRY IN PERSON, IN PRINT, ONLINE