ALERT LOGIC®

WHEN TECH IS NOT ENOUGH

Bringing Tools & Resources Together for Better Security Compliance

If you run a business that deals with sensitive customer data, we likely don't have to remind you of the regulations written to protect that data. But, reports of security breaches and non-compliance with these regulations are splashed across business pages every day:

Dixons fined £500K

by ICO for insufficient security that exposed 6.5 million customers' payment cards[1]

due to a lack of systemic protocols to protect against malware, which infected 5,000+ of the retailer's POS machines and allowed more than 5.6 million payment details and about 10 million non-financial records to be exfiltrated between July 2017 and April 2018.

British Airways faces $230M

GDPR fine for 2018 data breach[2]

after more than 500,000 web visitors were diverted to a fraudulent site where names, billing and email addresses, and payment information were harvested.

Marriott takes $126M

charge related to data breach[3]

after credit card and passport numbers of up to 500 million users were exposed when one of the hotelier's reservation systems was compromised by cyberattackers in 2014.[4]

Breaches and non-compliance can result in regulatory or industry penalties—including significant fines (see table)—and can have longer-term effects on a business's reputation and customer retention.

MAJOR PRIVACY & SECURITY FRAMEWORKS YOU SHOULD KNOW ABOUT

FRAMEWORK/ LEGISLATION	DETAILS	PENALTIES FOR NON-COMPLIANCE
CCPA (California Consumer Privacy Act)	Regulates sharing of personal information of California residents	Civil penalty of US$2,500 per violation or US$7,500 for each intentional violation
FISMA (Federal Information Security Management Act)	Enforces the requirement for U.S. agencies, vendors, and partners to implement cybersecurity protection protocols; based on NIST requirements	Potential penalties include censure by U.S. congress, a reduction in federal funding, and reputational damage
GDPR (General Data Protection Regulation)	Regulates the privacy and security of personal data of E.U. residents	Up to 4% of a company's annual global turnover or €20 million, whichever is higher
HIPAA (Health Insurance Portability & Accountability Act of 1996)	Provides privacy and security provisions for the use and disclosure of Protected Heath Information (PHI) of U.S. consumers	Based on level of negligence; from US$100–$50,000/violation (or per record) with a maximum of US$1.5 million/year
PCI-DSS (Payment Card Industry Data Security Standard)	Mandated by credit card brands to set technical and operational requirements for securing cardholder data	From US$5,000–$10,000/month, depending on the volume of clients and transactions affected, the level of PCI-DSS the company should be at, and the amount of time the company's been non-compliant
SOC 2 (System & Organization Control)	Auditing component of the American Institute of CPAs' Service Organization Control reporting platform; ensures the security, availability, and privacy of cloud-hosted consumer data	Up to 4% of total annual revenue
SOX (Sarbanes-Oxley Act)	U.S. federal law that regulates the use, holding, and alteration of corporate electronic records, including financial, accounting, and corporate disclosure	A corporate officer who doesn't comply or submits inaccurate certification—even if done mistakenly—is subject to a US$1 million fine and 10 years in prison. If wrong certification was submitted purposely, the fine can be up to US$5 million and 20 years in prison.

NOTE: Industry organizations have also created guidelines for protecting and preserving data and information:

- The International Organization for Standardization (ISO) developed the ISO Member Data Protection Policy to regulate the use of and access to personal data.
- The National Institute of Standards and Technology (NIST) developed their Cybersecurity Framework to help organizations to mitigate cybersecurity risk for critical infrastructure.

REGULATORY COMPLIANCE IS AN INCREASINGLY CHALLENGING MANDATE FOR MANY ORGANIZATIONS

Aside from the significant financial penalties meted out to organizations that are non-compliant, there are additional compelling reasons for keeping security and privacy controls up to regulatory standards. First and foremost is the desire to avoid the financial and consumer backlash that often occurs after cybersecurity attacks. But achieving and staying in compliance can be challenging, especially in cloud environments, where resources are constantly changing and a shared security responsibility model with cloud providers leads to a division of cybersecurity protection.

And while securing sensitive data is critical in achieving and maintaining compliance, a surprising number of organizations have still not updated their security and privacy controls and technology to meet compliance requirements. For instance, now almost two years after being introduced, many companies are still working to get their security controls and data protection projects in order to comply with GDPR requirements[5]—including some 72% of organizations surveyed by Capgemini for their 2019 "Championing Data Protection and Privacy" report.[6]

WHAT'S HOLDING ORGANIZATIONS BACK FROM ACHIEVING REGULATORY COMPLIANCE?

A number of interrelated factors make it difficult for organizations to meet compliance mandates with the tools and resources they have in-house, including:

- the significant investments necessary to achieve alignment with different compliance mandates[7] (especially funds put towards upgrading legacy IT systems, securing expert consultation and legal representation, and hiring trained professionals for key roles[8])
- the number and complexity of different, but often overlapping, legislations currently governing data security and protection (this is in addition to new regulations that will come into force in 2020, including Brazil's General Data Protection Law and India's Data Protection Bill)
- the ongoing cybersecurity talent shortage—with more than 4 million positions open around the world[9] and too few programs offering comprehensive training to develop and cross-train new practitioners[10]
- the evolving nature of the digital landscape, which leads to new and untested security issues that require continued knowledge-sharing that's just not taking place in the industry; this can result in higher rates of employee dissatisfaction and burnout and staff retention issues

Did you know?
Companies are allocating 14.3% on average of their IT budget to compliance.[13]

Yet, even in the face of these real business challenges, the costs of non-compliance can be 2.7 times higher than the investment necessary to meet regulatory mandates.[11] And numerous studies[12] have shown that the benefits of regulatory compliance are greater than first expected—including gaining a competitive advantage and increased consumer trust, a better brand image, and improved employee morale, not to mention improving IT systems and cybersecurity defenses.

The costs of non-compliance can be 2.7 times higher than the investment necessary to meet regulatory mandates.[14]

In this light, more companies are enlisting regulatory compliance technology (i.e., RegTech) to address some of their gaps in organizational expertise and provide necessary system controls, such as vulnerability management, intrusion detection, and endpoint protection, to help meet compliance requirements. (An additional benefit: when you start to map the security controls needed to meet all these rules, standards, and requirements, you'll quickly realize that some security controls often apply to multiple compliance projects.)

However, security controls and mapping are only one part of the solution that's needed to support compliance projects across multifaceted enterprises. Indeed, because organizations need to achieve compliance preparedness across multiple regulations and frameworks simultaneously, relying on technology alone will only get them part of the way to achieving greater peace of mind.

So, what's a well-intentioned, but lean-and-mean organization to do to up-level their regulatory compliance protocols and keep them working as new regulations get introduced? We recommend a "Tools+People Approach" to regulatory compliance.

TAKE A "TOOLS+PEOPLE APPROACH" TO IMPROVE SECURITY COMPLIANCE WITH FEWER DEDICATED RESOURCES

Instead of focusing solely on upgrading systems and infrastructure, we contend that a more effective and sustainable approach leverages a combination of technology and expertise to provide a superior defense against cyberthreats and bring increased peace of mind to businesses that struggle to find or dedicate staff to compliance projects. In fact, it's almost like having a virtual governance, risk, and compliance (GRC) resource without having to build and operate a GRC department from the ground up.

We've rolled out this approach with thousands of clients since 2002. With our award-winning SaaS security platform, coupled with a team of researchers and security analysts who deliver threat intelligence and expert response, we act as an extension of our clients' IT teams. This "Tools+People Approach" helps organizations determine which security controls apply across multiple compliance projects.

When companies use security tools plus expert staff support to gather threat intelligence and provide a human response to data security and protection issues, they're able to stay one step ahead of evolving compliance requirements, regulations, and standards without incurring the high costs of upgrading their own internal systems or hiring in-house security staff.

Does this sound like the right solution for your organization's security mandates? Learn how you can get better outcomes across your entire cybersecurity compliance program.

[1] https://www.theregister.co.uk/2020/01/09/dixons_store_group_fined_500000_by_ico_for_crap_security_that_exposed_56_millino_customers_payment_cards/
[2] https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
[3] https://www.wsj.com/articles/marriott-take-126-million-charge-related-to-data-breach-11565040121
[4] https://www.csoonline.com/article/3441220/marriott-data-breach-faq-how-did-it-happen-and-what-was-the-impact.html
https://www.reuters.com/article/us-usa-cyber-congress/marriott-ceo-apologizes-for-data-breach-unsure-if-china-responsible-idUSKCN1QO217
[5] https://www.symantec.com/blogs/expert-perspectives/gdpr-turns-1-many-companies-still-not-ready
[6] https://www.capgemini.com/championing-data-protection-and-privacy/?
[7] https://www.cio.com/article/3237147/regulatory-technology-innovating-compliance-and-your-business.html
[8] https://www.capgemini.com/championing-data-protection-and-privacy/?
https://www.forbes.com/sites/oliversmith/2018/05/02/the-gdpr-racket-whos-making-money-from-this-9bn-business-shakedown/#66465aa234a2
[9] https://www.isc2.org/Research/Workforce-Study#
[10] https://www.information-age.com/cyber-security-training-123474550/
[11] https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study
[12] https://www.capgemini.com/ca-en/news/championing-data-protection-and-privacy-report/#
[13] https://www.corporatecomplianceinsights.com/true-cost-compliance/
[14] https://www.globalscape.com/resources/whitepapers/data-protection-regulations-study

ALERT LOGIC®