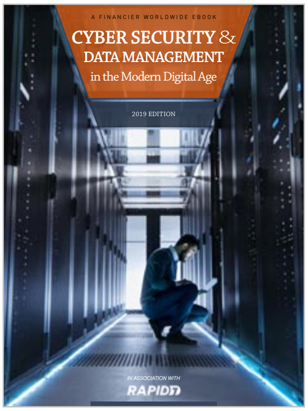


Published by Financier Worldwide Ltd
©2019 Financier Worldwide Ltd. All rights reserved.
Permission to use this reprint has
been granted by the publisher

■ **EBOOK** Cyber Security & Data Management in the Modern Digital Age 2019

COMPLIANCE AS A BY-PRODUCT OF GOOD SECURITY

Neil Campbell and Scott King at Rapid7 explore whether regulatory compliance can be achieved by establishing a robust cyber security framework. ■

SCOTT KING
Senior Director, Security Advisory Services
scott_king@rapid7.com

Scott King is the senior director of security advisory services for Rapid7. He has over 20 years professional work experience in the IT and cyber security fields. He brings a unique mixture of hands-on experience in incident response, penetration testing, forensics, operations, architecture, engineering and executive cyber leadership. Mr King has been a huge advocate for, and force behind, building better cyber security practices and approaches, providing comment and guidance for federal and state cyber legislation, giving presentations to boards of directors, providing testimony, and giving talks at industry conferences and trade shows.

NEIL CAMPBELL
Vice President, APAC Sales
neil_campbell@rapid7.com

Neil Campbell has spent more than 25 years specialising in cyber security, in global, regional and local roles, across law enforcement, consulting, telecommunications and managed security services organisations. Now leading Rapid7's sales team in APAC, Mr Campbell is focused on making a positive impact on cyber security outcomes at scale, as it is a problem that has to be addressed at scale in order to create sustainable change.

Q&A

COMPLIANCE AS A BY-PRODUCT OF GOOD SECURITY

Neil Campbell and Scott King at Rapid7 explore whether regulatory compliance can be achieved by establishing a robust cyber security framework.

Q. Could you explain how data protection and privacy laws are impacting the vast majority of organisations?

CAMPBELL: The vast majority of organisations have modest or no obligations with regard to data protection and privacy, as in many jurisdictions small businesses are either exempt from compliance or have a greatly reduced compliance burden. An example requires organisations with less than 250 employees to only keep internal records of processing activity, where such activity may put an individual's rights at risk; being in Australia, where organisations turning over less than A$3m per annum are exempt from the Privacy Act, albeit with some exceptions, and the recent amendment to the Privacy Act, requiring organisations to notify the government of data breaches. In the US, California pioneered data breach notification laws, which apply to all businesses – SB 1386, which came into effect in 2003 – and has recently passed the Consumer Privacy Act of 2018, which is due to come into effect in 2020 but will exempt most small to medium businesses from compliance. The US does not yet have federal data privacy or data breach reporting legislation. The challenge for organisations, both small and large, is in being aware of, and complying with, the data privacy and breach notification legislation that applies in the markets in which they conduct business. Organisations that collect the personal information of EU citizens must comply with the GDPR, regardless of their location. This has led to an ever-increasing burden on those organisations, as each new compliance requirement has its own specifics and subtleties, so it is not enough to comply with local legislation and assume that you will be covered for all other jurisdictions.

KING: These new laws are forcing companies to implement cyber security precautions in order to lessen the likelihood of a cyber intrusion. Businesses that have not historically invested in cyber protections or prepared for a breach are now forced to do so in order to protect themselves from the massive fines associated with privacy breach laws. Where the laws do not have a financial implication, and only require notification to impacted customers, the investment into cyber protections is much less, and more aligned to current business risk management philosophies, if any.

Q. To what extent have regulatory authorities stepped up their monitoring and enforcement efforts in this area, increasing the risks arising from non-compliance that companies face?

KING: This equates back to the early days of Payment Card Industry (PCI) compliance. Many companies then chose to pay the fine as compliance would be cost prohibitive. Most regulatory bodies do not have the enforcement teeth to truly drive better cyber risk management through massive fines. Where we have seen those occur, it is often designed to send a message to any other company ignoring the new laws. Over time, this will change or be challenged in court. We are still in the infancy of cyber regulations as many of the standards out there are largely ineffective in actually reducing cyber liability through proactive risk management.

CAMPBELL: Regulation tends to be only as strong as the history of penalties for non-compliance demands. The calculated view of compliance is that the cost of compliance is weighed against the penalties for non-compliance, with logic dictating that the lower cost choice is the one to go with. That view puts aside any thoughts of moral accountability but it is a good starting point for understanding whether a compliance regime will be effective or not. With penalties for various data privacy regulation and legislation ranging from an adverse ruling with no penalty up to forfeiture of 4 percent of global revenue, which is possible under the GDPR, the framework for strong deterrence is definitely in place. In January, Google was fined €50m for breaching the GDPR, and privacy activists have filed complaints under the GDPR against many of the US tech giants, so there may well be more large fines to come. It is fair to say that regulators around the world are increasing their focus on compliance, via investigation – generally as a result of a complaint – and increasing penalties, in order to ensure that compliance with data privacy legislation and regulation is seen as the sensible course of action for organisations.

Q. Given that cyber security features heavily in many data-related regulations, do companies often adopt the attitude that compliance equals a strong security programme? In your experience, is this a misconception?

CAMPBELL: It is tempting to believe that a strong security programme is equal to compliance with data privacy legislation, but that is far from the truth. Conversely, compliance does not necessarily equal strong security. I do think there has been confusion around this concept in the past, but CISOs from large organisations that I speak to understand that the two are very different. Compliance has very specific requirements, such as how customers are informed of their rights and what those rights are, or what records must be kept and how they must be communicated or made available for audit, or when and who to notify in the event of a data privacy breach. Having a strong security programme tends to mean that an organisation has a robust approach to protecting its digital assets. The right kind of programme to have in place is an effective risk management programme. This focuses first and foremost on the risks that an organisation faces, including regulatory and legislative compliance risks among many others, and drives the creation of security controls – including technology, standards and procedures resulting from policy created in response to an organisation's risks – that should encompass compliance as a part of an overall risk management strategy.

Q. To what extent can risk-driven cyber security drive compliance as a natural by-product?

KING: A risk-driven cyber security programme is based on industry best practices and, more importantly, frameworks. By adopting the underlying framework, it can easily be mapped to any cyber security compliance requirements. With the exception of ongoing evidence collection of the enforcement of cyber practices, that mapping allows a company to show its compliance and achieve a best practices programme. The other facet is that most compliance only applies to a portion of a company's systems and networks, whereas best practice, by its nature, applies to everything, including the systems and networks under a compliance obligation.

Q. What are the essential components of a risk-driven cyber security programme? What areas of the business should it encompass?

CAMPBELL: As an over-simplification, a risk-driven cyber security programme should consider all risks that impact on cyber security. A brief example of areas of risk includes insiders, competitors, government, regulatory, financial, operational and fraud. Risk management encompasses every aspect of the business, and touches IT assets more often than not, so the scope of the cyber security programme will be determined by the results of the organisation-wide risk management programme.

KING: Cyber risk is cross cutting and can impact any area of a company. As such, cyber risk should adopt the same risk calculator and impact decisions the rest of the company uses. This ensures common alignment and equal risk-based decision making. The essential components are the same for cyber as they are for enterprise risk: category, impact, likelihood and frequency.

Q. What advice can you offer to companies on successfully implementing risk-driven cyber security, and rolling it out across the organisation? What challenges and pitfalls might they need to overcome along the way?

CAMPBELL: The critical element here is that cyber security risk is considered as just another aspect of organisational risk management and managed as a part of that overall process. In that way, the relevance of the resultant risks and treatment plans is tied into the whole-of-organisation risk management context, which means that you are more likely to manage and resource your cyber security programme appropriately.

Q. How do you envisage cyber security and data protection

issues developing over the coming months and years? Do you believe companies need to maintain constant vigilance in this area, and continually update and enhance their security programme?

CAMPBELL: Cyber security is an exciting and challenging field because it is so dynamic. I sometimes use the AltaVista Firewall as an example to illustrate the changing nature of the internet and cyber security. AltaVista, which was really the forerunner to Google in terms of search, developed a firewall in the 1990s that had a particularly interesting feature. When the AltaVista Firewall detected that it was under attack, it could shut down the affected service or the entire firewall, as a preventative measure. This feature reminds me of the Peril-Sensitive Sunglasses from 'Hitchhiker's Guide to the Galaxy'. When the glasses detect that the wearer is in peril the lenses go completely black, so that the wearer does not have to see the terrible thing that is about to happen to them. Today, I cannot think of an organisation that would want to disconnect itself from the internet if its firewall was under attack. I can, however, imagine just how often the firewall would go offline, given the frequency of attacks that we see on the internet now. We have to accept that change is a given. Hopefully that change will include the United Nations (UN) ratifying a global treaty on data privacy and breach notification, in the spirit of the Universal Declaration of Human Rights. Having a UN-ratified treaty would give the world a framework under which to create consistent legislation to increase the coverage and reduce the complexity of data privacy and breach notification compliance. In the meantime, and it may be a very long meantime, organisations should remain vigilant in monitoring for changes in regulation and legislation, as well as the threats and risks that they face, while being prepared to rapidly update their security programme in response and sometimes even in anticipation.

Advance Securely with the Rapid7 Insight Cloud

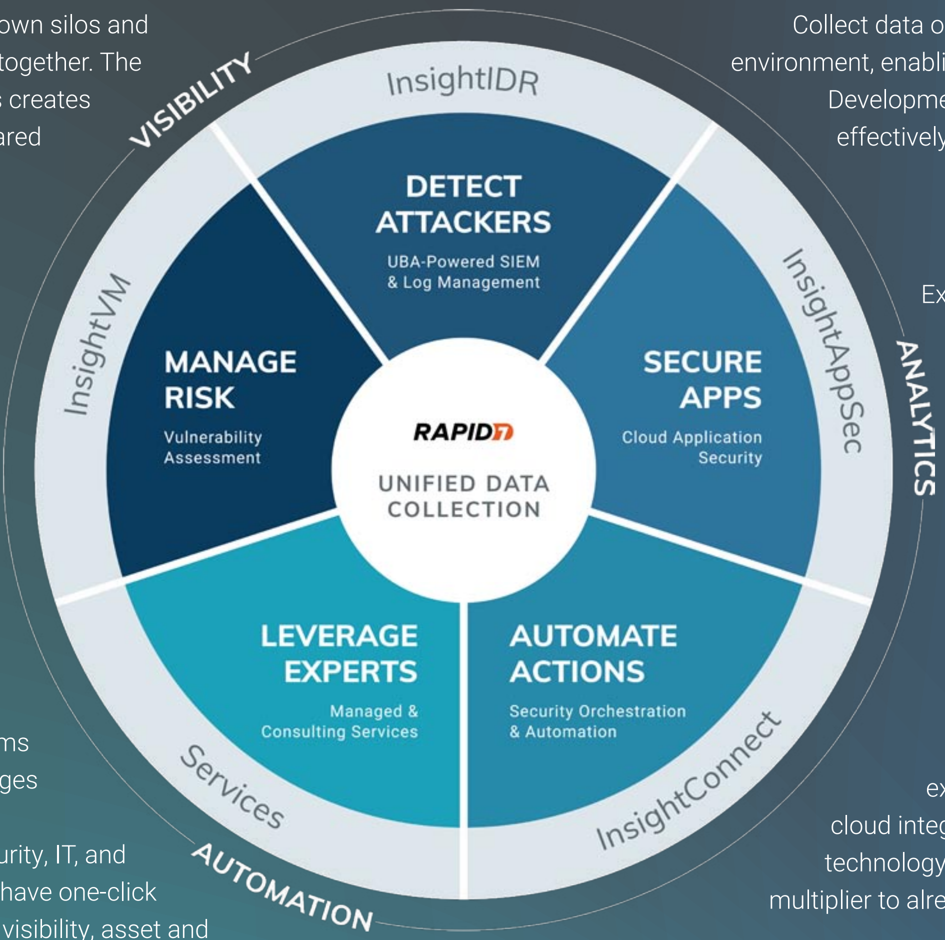
Reducing risk across your entire connected environment doesn't have to be complex. Try Rapid7 Insight for free at **www.rapid7.com/try/insight**.

Your Home for SecOps

It's time to break down silos and securely advance, together. The practice of SecOps creates an alliance and shared mission between Security, IT, and Development to make security an opportunity—not an obstacle.

How can you do it?

Rapid7 Insight is simplifying the complex through shared visibility, analytics, and automation that unite your teams around the challenges and successes of cybersecurity. Security, IT, and Development now have one-click access to network visibility, asset and application vulnerability management, threat detection and response, and orchestration and automation.



Unify Data Collection

Collect data once from across your IT environment, enabling your Security, IT, and Development teams to collaborate effectively as they analyze shared data.

Scale with Ease

Expanding your use of the Insight cloud to include multiple solutions is easy. Once your data collectors are installed, launching new Insight products is just a few clicks away

Integrate Seamlessly

Get faster analysis, prioritization, and remediation with your existing tools. The Insight cloud integrates with your existing technology stack, acting as a force multiplier to already-deployed solutions.

Ready to simplify your security?

Start your free Insight cloud trial at www.rapid7.com/try