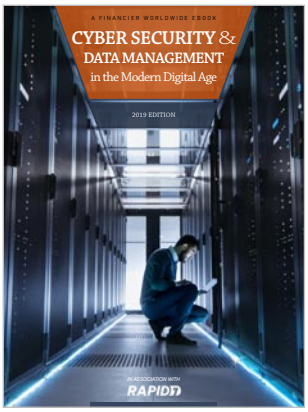



Published by Financier Worldwide Ltd


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

# SECURITY AS A BUSINESS PROBLEM

Scott King and Neil Campbell at Rapid7 offer an insight into why companies should approach cyber security as a broader business problem and also, 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

# SECURITY AS A BUSINESS PROBLEM

Scott King and Neil Campbell at Rapid7 offer an insight into why companies should approach cyber security as a broader business problem.

***Q. To what extent has the topic of cyber security been shifting up the leadership chain in recent years? How would you describe its ascent?***

**KING:** We have seen the security leader moving from the role of an SME reporting into IT, to the role of a business leader contributing to the direction of the company and the strategy of the business. This transformation is slow moving and the vast majority of companies still consider the role of a cyber security

leader to be in the IT organisation or within compliance. While this is true for many mid-size and smaller organisations, many larger companies have seen the value of bringing the security leader into increasing levels of responsibility and the benefits their perspective has on risk management and threats to the business.

**CAMPBELL:** With the increase in legislation around data privacy, protection and breach notification, the awareness that breaches are increasingly associated with espionage – both industrial and state-based – and the high media visibility breaches attract, cyber security has become a major consideration for governments, executive teams and boards around the world. The introduction of roles such as chief information security officer and chief privacy officer reflect that fact that leaders are recognising the importance of cyber security and the need for it to have one or more owners at an executive level within an organisation.

***Q. How would you characterise the level and nature of cyber risks currently facing businesses around the world?***

**CAMPBELL:** Cyber risks can range from unintentional disclosure of data by an employee or business partner, through things like insider threats from employees or contractors with political or financial goals, to external but also politically, financially or even competitively motivated attackers. The external attackers' methods may range from conducting automated, scan-based reconnaissance across large blocks of the internet in an attempt to find something interesting or useful to them, through to highly targeted, sophisticated and persistent attacks by determined criminals or nation states. I could go on, as there are many other sources of cyber risk that need to be considered. There are two main things to keep in mind when considering these cyber risks. The first is that every organisation's risks are unique to them, based on a number of factors including whether they hold or process data that is subject to data protection or privacy obligations, whether they create or hold intellectual property that is critical to the existence or success of that organisation, their level of dependence upon information technology, whether they rely heavily on internet-generated revenue, and so on. As in all forms of risk management, it is the frequency with which those risks are realised and the resultant impact on the organisation

that determines the appropriate level of priority and investment an organisation should allocate in order to manage those risks to acceptable levels. The second is that, as in many aspects of life, the 80:20 rule applies. The average organisation – if there can be such a thing – will be able to manage 80 percent of its risk with 20 percent of the theoretical total investment it could make in managing its risks. The hard part for every organisation is working out how much of the remaining 80 percent of the total theoretical investment it should make in order to manage the last 20 percent of the risks effectively. To illustrate that point, if an organisation invests in fundamental security controls, such as firewalls, end-point protection, multi-factor authentication, VPNs and patch management, along with all of the people and processes to run them, it will be protected against the vast majority of cyber risks that it face. It is then the organisation's unique risk profile that should determine how much of the remaining 20 percent of risks need to be managed appropriately.

**KING:** Risks have changed. Where once the risk was to worker productivity, now the risks have evolved into true financial impacts, whether from extortion, litigation or vast sections of busi-

ness downtime. This has allowed the security leader to quantify the potential impacts and justify projects and resources, but those businesses that continue to treat the risk haphazardly or discount it outright will undoubtedly incur a negative outcome that will change their perspective in the relative short term.

***Q. What recent, high-profile breaches have made it to the mainstream media and caught your attention? What insights can be drawn from these examples?***

**KING:** NotPetya – talk about a global wake-up call. This is unfortunately becoming the new norm. Chief executive officers and boards should draw their own conclusions based on examples like this to better inform their decision making around investment in cyber risk management. It is one thing to live on the edge and allow risk to exist, and completely another to discount it or believe compliance or insurance will address the true business impacts from a breach.

***Q. What are some of the common challenges that arise when discussing cyber security risks with boards and senior business***

***leaders? In your experience, what level of knowledge and understanding of these issues do corporate directors and executives tend to possess?***

**CAMPBELL:** The most common challenge is translating cyber security into a business-relevant context. Cyber security risks and controls are meaningless to a board unless they can be communicated in such a way that the risks, and the recommended changes to manage those risks, can be related back to the business.

**KING:** The largest challenge is a language barrier. Many cyber security leaders that have come up from entry level positions in the profession do not possess the business acumen or the perspective it takes to manage a profitable company. For those cyber security leaders that have rotated into the role, they typically have more business acumen, but lack true understanding of the cyber threat and associated risks, which lends to drawing misinformed conclusions as to the true liability. This is not an easy challenge to solve as the global workforce shortage for competent cyber security professionals continues to increase.

Corporate directors and executives in almost all cases should be recruiting cyber security board members that can participate in technology risk management and audit to inform the business as to its true risk.

***Q. How important is it to demystify what can often be deeply technical information, or vague 'legalese'? How can this be achieved?***

**CAMPBELL:** It is critical when the point of the discussion is to communicate clearly with stakeholders such as staff, executives, board members, media and so on. If you have a knee injury and you consult a surgeon to find out what the problem is and what the best way to treat it would be and that surgeon explains very precisely using detailed medical language, you are likely to be left very frustrated and wondering what has just been said. You would also be left hoping you can find another surgeon who can tell you clearly and plainly what the problem is, how they propose to fix it and what the risks of both treatment and non-treatment are. A cyber security professional who cannot communicate simply and in the right context is unlikely to be successful

in building the required trust and support to fulfil their role.

***Q. Given the outlook for rising cyber threats – and increasing liability for companies that fail to address them – what practical advice would you offer to business leaders on improving their understanding of cyber security in the digital age?***

**KING:** Business leaders need to qualify their cyber security risk and start quantifying the potential financial impacts of leaving those risks managed in their current state. This will allow informed decision making to help better prepare for a breach situation.

**CAMPBELL:** Whilst cyber security-related risks are relatively new, with threats evolving at a rapid pace, they are still just risks, which need to be understood and managed appropriately within every organisation. A strong culture of risk management must come from the board and executive team and be inculcated throughout the organisation from there. This is as true for an area such as legal risk as it is for cyber security risk. Business leaders need to ensure that they understand the basics of cyber

security, including how it fits into their overall risk management framework and what behaviours they, as leaders and employees, need to adopt in order to contribute and lead in the area of appropriate cyber security practices. Leaders can be tempted to consider themselves exempt from having to comply with cyber security practices, whereas they must be the exemplars.

RAPID7

# Advance Securely with the Rapid7 Insight Cloud

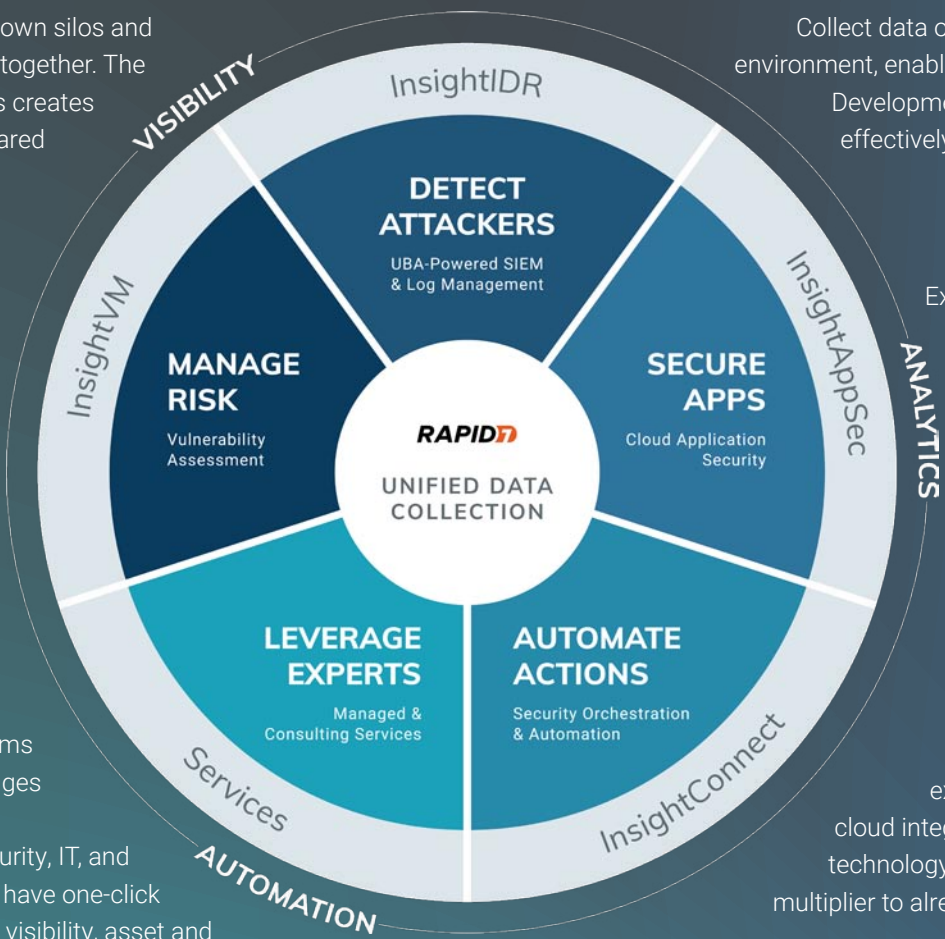
Reducing risk across your entire connected environment doesn't have to be complex. Try Rapid7 Insight for free at **www.rapid7.com/try/insight**.

### 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