FORREST™

Growing leaders of character who achieve extraordinary results™

Does Your Approach to Security Help or Hinder Your Business?

A new approach to security could generate savings as well as create a competitive advantage for your business. All that is required is a shift in perspective, and a focus on security risk management.

Phillip Halton
Writer and consultant on defence and security matters

The traditional business approach to the subject of security sees it as a "necessary evil." The security function is a cost-centre, and its role can seem to be to inhibit operations. To transform the security function from an overhead cost to a business enabler, a new perspective is required. Businesses should not think in terms of "having security," but instead should practice *security risk management*.

Risk exists as a natural and unavoidable consequence of our interactions with the world. While many might seek to avoid risk in their lives, in most cases this is not feasible. The financial and insurance sectors are examples of businesses that embrace risk at the core of their operations – and generate profit through their ability to take smart risks. The traditional approach to security has been to attempt to negate risk – this is a fool's errand. Instead, security risk management seeks to understand, measure and then mitigate risks to an acceptable level. Security risks are essentially nothing more than a sub-set of operational risk – and so should be approached as business problems to solve, not issues requiring exotic, non-business solutions.

The Common Approach to Security

Security functions tend to exist in "silos," focusing on the mantra of "prevent-detect-respond." This model is put into practice within a narrow sphere by security experts who are often "ex-something" – former police or military. This model hinges on the idea that security is an esoteric field of knowledge

that is removed from business operations. To put this knowledge into practice, businesses hire what amount to outsiders. Security professionals have supported this model for a number of reasons – their outsider status brings a degree of prestige, adds a touch of mystique to their work, and encourages a lack of scrutiny by business leaders. While this model works at a basic level, it misses the potential that an enlightened security function can unlock for a business.

The Security Risk Management Approach

The security risk management approach sees security risks in a different light. The security function is not something that can be isolated in a silo – it is a set of practices integrated throughout the business. To achieve this, the following approach can be used:

1. Identify Security Threats. At this stage, an exhaustive list of the security threats that the business faces is compiled. A security professional can assist with defining and categorizing security threats, but this activity cannot be conducted by a security team in isolation. Input from all functions is required to identify the potential threats – it takes an insider to understand the nuances of business operations and the threats involved.

2. Measure Security Risks. "Threat" and "Risk" are often used synonymously, but they are different concepts. Put simply, a "threat" is a negative event that could occur. "Risk" is a measure of the business impact of that threat – based on its likelihood, a consideration of the value of the assets at risk, and the businesses vulnerability to that particular threat. The same threat event could impact two businesses very differently – and so the measurement of the security risk environment requires a strong understanding of your own business operations. Although "risk assessments" are often conducted by security professionals in isolation, this can result in a skewed perception of the true risks posed by the threat environment.

3. Plan Mitigation Measures. Not all security risks can, or should, be mitigated. A zero-defect mindset must be avoided when considering security risks. Those threats that pose low risks to the business can be weathered without often expensive programs to "eliminate" them. For those threats that pose unacceptable risks, consideration should be given to the full gamut of potential mitigation measures, which should include non-security measures, as well. For example, insuring an asset might be much more cost effective than trying to secure it. The true risk from a security threat may be more reputational than financial – this would also suggest a non-security approach to mitigation. Even where security measures are put in place to mitigate risks, their cost and impact on business operations must be considered against the true risk posed to the business. All too often, high-cost security systems are put in place to protect low-value assets.

4. Monitor Implementation of the Plan. No plan can be allowed to run without monitoring its effectiveness. The use of metrics is not as common in the security field as it is in other parts of business, but it is a highly valuable means to track the effectiveness of a security risk mitigation plan. It also serves a second purpose – it translates security activities into a language and format that is easily read and understood by business professionals, while forcing security professionals to think in business terms.

Finding the "Sweet Spot"

Done well, the approach outlined above will help to focus the security function on the things that are important to the business while filtering out the "noise" generated by the threat environment. The key to developing a successful security risk management strategy is to ensure that business leaders are engaged and consider the security function in terms of risk.

As an example, a security professional might focus on achieving a 0% loss rate to some aspect of the business. Objectively, this figure appears to be a positive one. But a business-integrated risk approach forces consideration of what the cost to achieve this loss rate is, both in terms of expenditures and operational "friction." It then allows the business to consider the relative cost of

achieving a higher loss rate – and the resulting total cost. Particularly for non-critical business functions, it may be more cost- and operationally-effective to accept a 1–2% loss rate (or even higher) than to achieve a lower one. Having key conversations with business leaders about security will help to determine the *acceptable* level of risk – which is the "sweet spot" for any business to achieve.

Security as a Competitive Advantage

There are many means that a business may use to gain competitive advantage over other businesses. Security risk management is rarely considered as one of them. An efficient security risk management strategy can represent a cost-savings over traditional approaches and remove needless impediments to operations. An effective security risk management strategy can also deter or deflect security threats onto competitors, creating an uneven playing field and resulting advantage.

Conclusions

The security risk management process can unlock hidden value for a business but, to do so, the security function must be fully integrated into business operations. This includes areas where security is seldom considered – such as business development activities and mergers and acquisitions.

Security will always be a cost-centre – but done well, it will secure key business functions and assets to the degree necessary, while not acting as a clunky drag on operations. To achieve this, security professionals must also be business professionals, able to understand the business at a functional level and to operate comfortably within it.

By comparing your business' current security practice with the steps outlined above, you will be able to gauge how far removed you are from a security risk management approach – and how much potential gain can be had by implementing it.

Phillip Halton is a writer and consultant on defence and security matters with over twenty years of experience. He combines a military background with experience working in the humanitarian sector, with multi-national businesses, and for various governments – with risk and security management as the thread tying his many experiences together. Phillip holds a Master's degree from the Royal Military College. He has worked and travelled in over sixty countries across five continents. This is Phillip's first guest-writer appearance with Forrest. Phillip can be reached via Michael Clark, Director, Sales & Marketing, mclark@forrestandco.com.

Forrest & Company is an organizational trans-formation firm. We are experts in identifying, developing and releasing the potential in leaders and their organizations. For over 25 years, Forrest's team of skilled consultants, facilitators, coaches, and designers have grown the capabilities and effectiveness of more than 30,000 leaders and their organizations worldwide..

www.forrestandco.com

0002